Do you bend or break?

Preventing Online Banking Fraud Victimization Through Online Resilience

Jurjen Jansen

Do you bend or break?

Preventing online banking fraud victimization through online resilience

Jurjen Jansen

Thesis, Open University of the Netherlands

ISBN: 978-94-6233-960-6

Cover design by Evelien Jagtman (www.evelienjagtman.com)

Printed by Gildeprint (www.gildeprint.nl)

The studies presented in this thesis are part of the Dutch Research Program on Safety and Security of Online Banking. This program is funded by the Dutch banking sector (represented by the Dutch Banking Association), the Police Academy and the Dutch National Police.

Do you bend or break?

Preventing online banking fraud victimization through online resilience

PROEFSCHRIFT

ter verkrijging van de graad van doctor

aan de Open Universiteit

op gezag van de rector magnificus

prof. mr. A. Oskamp

ten overstaan van een door het

College voor promoties ingestelde commissie

in het openbaar te verdedigen

op vrijdag 22 juni 2018 te Heerlen

om 16.00 uur precies

door

Jurjen Jansen

geboren op 21 september 1983 te Sneek

Promotor

Prof. dr. W.Ph. Stol, Open Universiteit

Co-promotor

Dr. N. Kop, Politieacademie

Leden beoordelingscommissie

Prof. dr. E. Giebels, Universiteit Twente

Prof. dr. E.W. Kolthoff, Open Universiteit

Prof. dr. C.J. de Poot, Vrije Universiteit Amsterdam

Dr. P.G. van der Velden, CentERdata Instituut voor dataverzameling en onderzoek

Dr. J.A. van Wilsem, Ministerie van Justitie en Veiligheid; WODC

Contents

GENERAL INTRODUCTION

1 Human aspects of online banking safety and security 9
1.1 Introduction 10
1.2 Context 13
1.3 Objectives and research questions 18
1.4 Scope and theoretical foundations 20
1.5 Relevance 25
1.6 Contents of the thesis 33

PART I: RISK PERCEPTION AND ONLINE BANKING FRAUD VICTIMIZATION

2 End-user perceptions of the safety and security of online banking 35
2.1 Introduction 36
2.2 Theory 37
2.3 Method 39
2.4 Results 44
2.5 Conclusion and discussion 47

3 How people help fraudsters steal their money 51
3.1 Introduction 52
3.2 Theory 52
3.3 Method 53
3.4 Results 55
3.5 Conclusion and discussion 63

4 Phishing and malware attacks on online banking customers 71
4.1 Introduction 72
4.2 Theory 73
4.3 Method 74
4.4 Results 76
4.5 Conclusion and discussion 82

5 Coping with cybercrime victimization 87
5.1 Introduction 88
5.2 Theory 90
5.3 Method 95
5.4 Results 97
5.5 Conclusion and discussion 106

PART II: PRECAUTIONARY ONLINE BEHAVIOUR

6 Comparing models to explain precautionary online behavioural intentions .. 117
6.1 Introduction 118
6.2 Theory 120
6.3 Method 124
6.4 Results 128
6.5 Conclusion and discussion 129

7 Testing a model of precautionary online behaviour 133
7.1 Introduction 134
7.2 Theory 136
7.3 Method 140
7.4 Results 143
7.5 Conclusion and discussion 150

8 Guarding against online threats: Why enterpreneurs take measures..... 159
8.1 Introduction 160
8.2 Theory 161
8.3 Method 164
8.4 Results 166
8.5 Conclusion and discussion 170

9 The design and evaluation of a theory-based intervention against phishing 175
9.1 Introduction 176
9.2 Theory 179
9.3 Method 183
9.4 Results 194
9.5 Conclusion and discussion 202

GENERAL CONCLUSION AND DISCUSSION

10 Improving the safety and security of online banking 209
10.1 Introduction 210
10.2 What are the perceptions of end users regarding the safety and security of online banking? 210
10.3 How can online banking fraud victimization be explained? 212
10.4 How can precautionary online behaviour of end users be explained and improved? 214
10.5 Theoretical and practical implications 215
10.6 Limitations 238
10.7 Concluding remarks 241

References 243
Appendix I: Outline research program 263
Appendix II: Interview data 264
Appendix III: Instrument private customers 265
Appendix IV: Instrument corporate customers 269
Appendix V: Instrument internet users 271
Summary 275
Samenvatting (summary in Dutch) 281
Dankwoord (acknowledgements in Dutch) 289
Curriculum vitae 292
Publications 293

GENERAL INTRODUCTION

CHAPTER 1

Human aspects of online banking safety and security

1.1 Introduction

'Computer insecurity is inevitable. Technology can foil most of the casual attacks. Laws can deter, or at least prosecute, most criminals. But attacks will fall through the cracks. Networks will be hacked. Fraud will be committed. Money will be lost.' This somewhat dark image of the digital society painted by Bruce Schneier (2000, p. 367) – an internationally renowned security technologist – is a reality that we will have to accept. However, we can contribute to making this dark reality somewhat brighter. An important contribution lies in making the weakest link in information security more secure. This thesis contributes to this effort in the context of online banking by studying fraud cases and the role of end users. More explicitly, the overall objective of the studies presented in this thesis is to find ways to improve the safety and security of online banking from an end-user perspective.[1]

The world we live in is becoming more networked and connected (Van Dijk, 2012). Services offered to customers, such as retail and government services, are increasingly provided online. This also counts for banking services, the context of this study. The digital revolution offers opportunities to end users in numerous ways. However, these advantages can be overshadowed by insecurity and fear of threats, such as the risk of losing money and privacy infringements.

Technological advances do not always result in better security in technical environments (Parsons, McCormac, Butavicius, & Ferguson, 2010). The internet was not designed with security in mind, it was designed for utility only (Purkait, Kumar De, & Suar, 2014). This 'utility' is, however, also used or misused by perpetrators, and so internet users fall victim (Bossler & Holt, 2009; Van Wilsem, 2011b), which may consequently lead to all kinds of harm.

Harm is not only done to individuals. Security issues, such as data breaches, distributed denial-of-service-attacks[2] or compromised systems, can also have negative effects on businesses, the economy and society at large. Besides financial damages, the effects of cyberattacks may lead to reputational damage and loss of goodwill and trust. Therefore, online safety and security are vital aspects in the digital society.

Ensuring online safety and security is not an easy task, however, as it can easily be compromised – either accidentally or deliberately (Furnell & Clarke, 2012).

[1] This study is one of four studies in the Dutch Research Program on Safety and Security of Online Banking. This program is outlined in Appendix I.

[2] A distributed denial-of-service-attack or DDoS-attack is a deliberate attack by which massive amounts of data are sent to block their intended users' access to systems, networks or services (Van der Hulst & Neve, 2008).

Perpetrators can use a range of tools in deliberate attacks, of which two are central to this thesis: phishing and malware attacks. Reports of such attacks are frequently mentioned in the news, both within and beyond the online banking context. An example of the former is a news story about perpetrators being arrested in Amsterdam who stole over 400,000 euros by means of phishing attacks.[3] An example of the latter is a news message describing that a spear-phishing attack was used as a preparatory act trying to influence the American presidential election in 2016.[4]

In terms of the safety of online banking, banks obviously have an important role in securing this online service. However, cyberattacks form a societal problem, which means that responsibility cannot be attributed to banks only (NVB, 2013). Hence, combatting cyberattacks requires a joint approach where multiple organisations, such as internet service providers, telecommunications companies and governmental agencies, bundle their forces. End users also play an important role. Moreover, end users are considered to be the Achilles heel for achieving online security (Furnell, Jusoh, & Katsabas, 2006; Liang & Xue, 2010; Ng, Kankanhalli, & Xu, 2009). Therefore, it is important for end users to become online resilient and 'bend' with these developments. This is necessary to stop people from 'breaking' and potentially becoming victims of online banking fraud.

When thinking about cyberattacks and cybersecurity, it is obvious to make associations with technical issues, such as technical security measures and fraud prevention and detection systems. This is, for example, also evident in the European Commission's cybersecurity strategy, which has a strong focus on technical aspects (EC, 2013). As far back as in 2001, Sasse, Brostoff, and Weirich (2001) observed that human aspects of information security are easily ignored, while humans are perceived to be the weakest link in the information security chain. However, as of late, human aspects gain more attention, because security fundamentally affects more people (Furnell & Clarke, 2012).

Furthermore, a great portion of cyberattacks are targeting end users (Furnell & Clarke, 2012). As a consequence, end users often cause security breaches, for example, when they are persuaded to click on a hyperlink in a phishing e-mail, enter personal information on a phishing website or open an infected attachment

[3] Nu.nl (2016). *Amsterdamse phishing-bende stal ruim vier ton via internetbankieren* [Amsterdam phishing gang stole more than 400,000 euros through online banking]. Retrieved from http://www.nu.nl/amsterdam/4284493/amsterdamse-phishing-bende-stal-ruim-vier-ton-via-internetbankieren.html

[4] Lipton. E., Sanger, D. E., & Shane, S. (2016). *The perfect weapon: How Russian cyberpower invaded the U.S*. Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

(Hong, 2012; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). Human factors, such as cognitive abilities and risk perceptions, impact end-user behaviour, which in turn influences the effectiveness of information security (Parsons et al., 2010; Rhee, Kim, & Ryu, 2009). Besides, end users are the ones that interact with computer or information systems, making the human factor an important issue by definition. Although a multidisciplinary perspective is needed to cope with online threats and vulnerabilities – as these often have multidimensional characteristics – this thesis adopts an end-user perspective on the safety and security of online banking.[5] This study accordingly falls within the domain of behavioural information security research, which is part of the broader information security field (Crossler et al., 2013).

Another reason to focus on end users is that technical security alone is not capable of guaranteeing the safety of online banking (Arachchilage & Love, 2014; Furnell & Clarke, 2012; Herath & Rao, 2009). Although basic security hygiene should be a precondition before interacting online and provides to a certain extent a barrier against technical attacks (NCTV, 2013), it cannot always prevent an end user from contracting a malware infection, nor can it prevent an end user from disclosing sensitive information to a perpetrator when persuaded to do so. Davinson and Sillence (2014) state in this regard that end users play an integral role in reducing succesfull fraudulent cyberattacks. How far end user responsibility should go is not under discussion in this thesis. The bottom line is that end users should be able to cope with threats aimed at online banking.

In sum, this thesis provides insight into the perceptions of end users regarding online banking safety, security and fraud victimization, and into the human aspects that influence end users so that they are cautious when online. Currently, not much work has been done on studying the human aspects of behaving cautiously when online and protecting end users from cyberattacks (Arachchilage & Love, 2014).

The remainder of this chapter is structured as follows. In Section 1.2, the context of the thesis is introduced. Section 1.3 continues with the goals and research questions that are central to this thesis. In Section 1.4, the scope and theoretical foundations are emphasised. Section 1.5 presents the relevance of

[5] A focus on the end user consequently means that less attention is paid to the cyber resilience of financial institutions (DNB, 2016) or the (technical) preconditions of safety and security of online banking, such as confidentiality, integrity and availability (the C.I.A. triangle), quality management systems (e.g., ISO 27001) and the internal and external security systems banks have in place and their design and usability, such as fraud detection systems and two-factor authentication.

the different studies conducted for this thesis. Finally, the content of the thesis is presented in Section 1.6.

1.2 Context

In this section, the subjects of the thesis are presented in more detail. First, the broader context of online banking is introduced (Section 1.2.1). Second, the narrower context of online banking fraud is highlighted (Section 1.2.2).

1.2.1 Online banking

One of the major innovative developments of recent times is the internet. The internet offers many opportunities to people as they can, for instance, communicate and do business with one another 24/7. For banks, the internet has provided opportunities to expand their services. With digital payments in general – and specifically online banking – banks created an alternative in which banking activities take place. This alternative makes it possible for people to arrange banking activities in a faster, cheaper way in any place at any time, as long as an internet connection is available.[6] Thus, online banking refers to banking via the internet using a device selected by the customer, including desktop and laptop computers, smartphones and tablets. In the context of this study, online banking is limited to online payments, online transfers and checking the account balance online.[7]

Compared to the traditional ways of arranging banking activities, online banking has some unique characteristics. Yousafzai, Pallister, and Foxall (2003) indicate that online banking is characterised by (a) an extensive use of technology; (b) a distant and impersonal online environment; and (c) an implicit uncertainty of using an open technology infrastructure for financial transactions. Where the relation between the bank and its customers might have been closer in the past (human-to-human), now this relationship is characterised by a separation of place and time (human via system-to-system). These characteristics are also applicable to the broader e-commerce spectrum as opposed to traditional commerce (Pavlou, 2003).

The results presented in this thesis are applicable to the Dutch online banking situation and may not necessarily be generalisable to other countries. In 1997, only a few years after the first public internet service provider was founded in the Netherlands, online banking via the World Wide Web was introduced in the

[6] Note that other forms of digital payment systems, such as counter payments (at physical stores), cash withdrawals from ATMs, and digital currencies are outside the scope of this study.

[7] Note that other activities that might fall under the scope of online banking, such as investments, mortgages and insurances, are outside the scope of this study.

Netherlands.[8] Twenty years later, 85% of the Dutch population aged 16 and over make use of this service (Eurostat, 2016). It seems, however, that the age group 65 years and over is lagging behind in the uptake of online banking with 44% users.[9] Together with the Nordic countries, the Netherlands is one of the frontrunners when it comes to the adoption of online banking.

The large adoption rate can be explained by several reasons. For the Dutch context, an important reason lies in the internet coverage rate, which is high in the Netherlands. In 2015, 91% of all households had access to the internet (CBS, 2016a). The adoption of online banking is also helped by banks that have closed down local bank offices[10] and that discourage the analogue ways of conducting banking businesses because they have stopped offering those services or have raised the costs.[11] In this respect, online banking adoption may be evaluated as a fait accompli. General indicators for online banking adoption – which are also relevant outside the Dutch context – include the previously mentioned unique characteristics of online banking that appeal to many people. Additionally, there are also customer-specific factors that affect the adoption of this self-service technology, for instance, having an optimistic attitude towards technology and the individual's innovativeness (Yousafzai & Yani-de-Soriano, 2012).

End users can install banking apps to access their bank accounts on mobile devices (smartphone and tablet). This is often referred to as mobile banking, a form of online banking that has been introduced in the Netherlands in 2011.[12] In 2016, around five years after its introduction, 63% of the Dutch population used mobile banking.[13] Although mobile banking comprises some differences, such as downscaled authentication, less functionality and physical places where bank

[8] Grinsven, L. van (1997). *Rabo eerste in race naar het net* [Rabobank first in race to the internet]. Retrieved from http://www.volkskrant.nl/wetenschap/rabo-eerste-in-race-naar-het-net~a487746/

[9] Unie KBO (2015). *Ruim een miljoen senioren bankiert nog niet online* [More than one million seniors are not yet banking online]. Retrieved from http://www.uniekbo.nl/nieuws/default.asp?page=detail&id=1329

[10] Den Hollander, E. & Vogels, P. (2014). *De bank? Daar komt bijna geen mens meer* (The bank? Almost no one goes there anymore). Retrieved from http://www.ad.nl/economie/de-bank-daar-komt-bijna-geen-mens-meer~a799627f/

[11] Hofs, Y. (2012). *Nooit meer een acceptgiro* [Never an acceptance giro again]. Retrieved from http://www.volkskrant.nl/archief/nooit-meer-een-acceptgiro~a3283088/

[12] Banken.nl (2011). *ING lanceert Mobiel Bankieren app voor smartphone* [ING launches mobile banking app for smartphones]. Retrieved from http://www.banken.nl/nieuws/4/ing-lanceert-mobiel-bankieren -app-voor-smartphone-en-tablet

[13] ING (2017). *Mobile banking, shopping and payments to surge in the next 12 months*. Retrieved from https://www.ezonomics.com/pdf/Mobile_Banking_release_FINAL.pdf

accounts may be accessed, no distinction is made between online and mobile banking in this thesis because they both involve similar uncertainties and risks, such as cybercriminals attacking mobile networks and intercepting personal information or using malware to obtain credentials (Zhou, 2012). However, as it stands now, online banking on mobile platforms is not attacked as often as online banking on desktop and laptop systems.[14]

1.2.2 Online banking fraud

According to the Dutch Banking Association, Dutch banks provide high levels of security for their products and services (NVB, 2013). This is necessary in order for digital payment systems[15] to operate as safely and smoothly as possible. Moreover, (digital) payment systems are considered one of the critical infrastructures of our society. An attack on these infrastructures may cause social disruption (Van der Hulst & Neve, 2008). When such attacks are carried out using information and communication technology they are called cyberattacks or cybercrime. The World Economic Forum evaluates cybercrime as the third most serious global risk considering the combination of its likelihood and impact, after fiscal crises and structural unemployment or underemployment (WEF, 2016).

The Dutch Banking Association defines two types of cybercrime with regard to digital payment systems: (1) targeted at negatively influencing the availability of digital payment systems; and (2) targeted at fraud with online banking and/or debit cards (NVB, 2013). Because this study concentrates on end users, the former is not taken into account and the focus is on the latter, more specifically on online banking fraud.[16]

Online banking fraud is part of the increasing extent, frequency and diversity of cybercrime. These events, combined with a rise in the use of electronic systems to store personal data, make information security an important asset in the 21st century. Therefore, it is imperative to better understand the effectiveness of security measures, but also laws, policies and strategies that deal with protecting and combatting cybercrime, and the motivations and crime scripts of cybercriminals. Although the idea of tricking people for financial profit is not

[14] Interview with a security architect from a Dutch bank (personal communication, April 23, 2014).

[15] A payment system is a 'set of instruments, procedures, and rules for the transfer of funds between or among participants; the system includes the participants and the entity operating the arrangement' (Bank for International Settlements, 2012), retrieved from http://www.bis.org/cpmi/publ/d00b.htm?&selection=49&scope=CPMI&c=a&base=term

[16] Note that other relevant crimes targeting end users, such as skimming and debit card fraud, are outside the scope of this thesis.

new, the characteristics of the internet make it more convenient for perpetrators (Furnell, 2008a). Williams (2015, p. 56) argues that online fraud is 'the most prevalent acquisitive crime in Europe.' The types of online banking fraud relevant in this thesis are limited to phishing and malware attacks.[17]

Phishing – a type of social engineering – is the process of retrieving personal information using deception through impersonation (Lastdrager, 2014). Phishing often starts with a deceitful e-mail, but also fake websites and fraudulent phone calls are applied to intercept user credentials. Malware – a type of technical engineering – is the infection of a computer system with malicious software, including viruses, worms, Trojan horses and spyware, for the purposes of carrying out the harmful intentions of an attacker (Moser, Kruegel, & Kirda, 2007). Examples of financial malware include Zeus, SkyEye and Citadel (Marinos, 2013). The aim of the perpetrator is to deceive the end user or the system used for online banking in order to obtain user credentials and/or to gain control over end users' devices. Perpetrators use these credentials to access a victim's online bank account and to validate money transfers on behalf of the victim. In short, the issues regarding the safety and security of online banking are limited to the integrity of transactions.

A sensitive issue regarding phishing and malware attacks on online banking is that security is compromised on the customer side. From a technological perspective, the bank's capabilities and control end at a given point. For example, banks cannot control end users' behaviours or their devices and infrastructure. From the perspective of making the online banking customer more resilient, the relevant questions then concern how to encourage them to take precautionary measures within their own domain, and to what extent that can be expected from customers, as some measures might be complicated and technical. Another important question is how to ensure that customers are cautious and alert in their behaviour, and continue to be so, also with regard to new developments and types of attack on online banking. These questions are relevant because customers or end users form an essential link in the information security chain.

During the preparation phase of this research project, attacks on online banking were targeted more at end user than at banks.[18] That end users are attacked more often nowadays does not mean that banks are not targets anymore. Consider, for example, the theft of a billion dollars by hacker group Carbanak in

[17] Note that both attack types can also be combined in a single attack (Aaron, 2010).

[18] De Volkskrant (2013). *Bankoverval komt nauwelijks nog voor* [Bank robberies hardly occur anymore]. Retrieved from http://www.volkskrant.nl/archief/bankoverval-komt-nauwelijks-nog-voor~a3393520/

2015.[19] In this phase, the number of reports about online banking fraud made by the Dutch Banking Association was at its highest level, with respectively 35.0 and 34.8 million euros of direct financial damages in 2011 and 2012.

Since 2013, the reported fraud figures have been declining in the Netherlands.[20] Various sources report that this decline is due the banks doing a good job in detecting fraudulent attacks in their systems and customers who are more aware of such attacks.[21] Furthermore, online banking fraud can be considered a marginal issue when placing it in perspective. In the Netherlands, about 3 billion transactions are made using online banking. These transactions represent a total value of 3,200 billion euros (NVB, 2013). Also compared with indications of other fraud types in the Netherlands (PwC, 2013), such as bankruptcy fraud (1,300 million euros), insurance fraud (900 million euros) and investment fraud (500 million euros), online banking fraud may seem to be a minor issue.

Although the fraud figures tend to decline, and the amounts that are stolen are relatively small, the cybercrimes that are studied are still a considerable problem that internet users need to deal with both within and beyond the scope of online banking (APWG, 2015). In the United Kingdom, for example, online banking fraud figures have increased from 2011 onwards.[22] Examples of Dutch organisations whose names are misused in phishing attacks besides banks include Bol.com,[23] PostNL[24] and Booking.com,[25] but also government bodies

[19] Infosecurity Magazine (2015). *Miljard dollar gestolen in grootste digitale bankroof aller tijden* [One billion dollars stolen in biggest digital bank robbery ever]. Retrieved from http://infosecuritymagazine.nl/2015/02/15/miljard-dollar-gestolen-in-grootste-digitale-bankroof-aller-tijde/

[20] Nederlandse Vereniging van Banken (2016). *Veiligheid en fraude* [Safety and fraud]. Retrieved from https://www.nvb.nl/feiten-cijfers/992/veiligheid-fraude.html

[21] Financieel Dagblad (2015). *Bank en consument dringen samen cybercrime terug* [Banks and customers curb cybercrime together]. Retrieved from https://fd.nl/economie-politiek/1102358/bank-en-consument-dringen-samen-cybercrime-terug

[22] Financial Fraud Action UK (2016). *Fraud the facts 2016: The definitive overview of payment industry fraud.* Retrieved from https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/Fraud-the-Facts-A5-final.pdf

[23] Security.nl (2015). *Bol.com waarschuwt voor nepmails* [Bol.com warns about fake e-mails]. Retrieved from https://www.security.nl/posting/451688/Bol_com+waarschuwt+voor+nep-mails

[24] NOS (2014). *PostNL-phishers: Kwart miljoen euro buit* [PostNL phishers: Quarter-million euros looted]. Retrieved from http://nos.nl/artikel/2000220-postnl-phishers-kwart-miljoen-euro-buit.html

[25] NOS (2014). *10.000 klanten Booking.com slachtoffer phishing* [10,000 Booking.com customers victimised by phishing]. Retrieved from http://nos.nl/artikel/2010287-10-000-klanten-booking-com-slachtoffer-phishing.html

such as the Dutch Tax and Customs Administration[26] and the Central Fine Collection Agency (CJIB).[27] The Fraud Helpdesk stated that, in 2015, Dutch internet users reported 123,000 phishing e-mails and damages amounting to 822,000 euros were suffered by nearly 500 victims.[28] The Dutch National Cyber Security Centre also notes that phishing and malware are still important issues in the Netherlands (NCSC, 2015). Hence, studying how to make end users more resilient against such attacks remains an important priority.

1.3 Objectives and research questions

The objective of this study is to improve the safety and security of online banking from an end-user perspective. In other words, it deals with the question of, and consequently how, online banking fraud victimization can be reduced. The central question is formulated as follows: *To what extent can the safety and security of online banking be improved from an end-user perspective?* In order to achieve the research objective, i.e., to answer the central research question, the following subdivision was made: (1) studying end-user perceptions of the safety and security of online banking; (2) studying online banking fraud victimization and coping mechanisms; and (3) studying precautionary online behaviour and motivations for that behaviour. Each part adopts its own main research question and sub-questions that contribute to answering the central research question.

1: What are the perceptions of end users regarding the safety and security of online banking?

   a. What are the perceptions of end users regarding threats to online banking?
   b. What factors determine end-users' risk perceptions of threats to online banking?
   c. To what extent do end users trust online banking?
   d. How are end users confronted with online banking threats?

[26] Telegraaf (2016). *Belastingdienst waarschuwt voor phishing* [Dutch Tax and Customs Administration warns about phishing]. Retrieved from http://www.telegraaf.nl/dft/geld/belasting/25305262/__Belastingdienst_waarschuwt_voor_phishing__.html

[27] NOS (2014). *CJIB: Betaal nepverkeersboete niet* [CJIB: Do not pay fake traffic fine]. Retrieved from http://nos.nl/artikel/667735-cjib-betaal-nepverkeersboete-niet.html

[28] Fraudehelpdesk (2016). *Verdubbeling slachtoffers internetoplichting* [Number of online scam victims doubles]. Retrieved from https://www.fraudehelpdesk.nl/nieuws/verdubbeling-slachtoffers-internetoplichting/

2: How can online banking fraud victimization be explained from an end-user perspective?

a. How and why do end users become victims of online banking fraud?
b. What end-user characteristics can be identified that increase the chance of online banking fraud victimization?
c. What are the effects and impact of online banking fraud victimization?
d. How do victims cope with online banking fraud victimization?

3: How can precautionary online behaviour of end users be explained and improved?

a. What theoretical models can explain precautionary online behaviour?
b. What are the predictors of precautionary online behaviour?
c. To what extent do the predictors of precautionary online behaviour differ between subgroups (gender, age, and education level)?
d. To what extent can predictors of precautionary online behaviour be influenced in order to improve end-user behaviour?

This thesis embraces various research methods that are used to study the research problems in question. In Table 1.1, a method matrix is presented which visually demonstrates the research methods that are used to answer the sub-questions. Besides the methods outlined below, which are described in more detail in the following chapters, each study started with a careful examination of the literature. In addition, interviews were conducted with fourteen key figures from the banking sector and police organisation at the start of the project. These were used to familiarise with the context at hand, but they were not processed for the purposes of the thesis.

Table 1.1: Method matrix

Research questions / Methods	Survey private customers (N = 1,200)	Case analyses bank files (N = 600)	Interview fraud victims (N = 30)	Survey corporate customers (N = 1,622)	Experiment internet users (N = 768)
1a-1d	X				
2a		X			
2b-2d			X		
3a-3b	X			X	
3c	X				
3d					X

Note that although end users are primarily limited to private customers of banks or internet users in general, corporate customers are included in some of the

studies that are presented later on. The rationale was that about 50% of financial damages due to online banking fraud is caused through attacking corporate customers.[29] Corporate customers mainly comprised self-employed entrepreneurs and in a few instances small and medium-sized enterprises, foundations and associations. This target group is becoming more of a target for cybercrime as they deal with larger sums of money than private customers and often lack the financial capacity that larger businesses have to hire cybersecurity professionals.[30]

The rationale to only include self-employed entrepreneurs and smaller enterprises is that the behavioural component is key. Primarily focusing on these types of customers gave the best guarantee that research participants from a corporate background were responsible for managing (i.e., implementing and maintaining or outsourcing) their information security and conducting their online banking activities. With larger businesses, it would be more difficult to study user behaviour or to target the right person in the first place, as it is often not clear from an external perspective which employee is responsible for what actions. Moreover, larger businesses often have other types of relationships with their bank and also use other types of services.

1.4 Scope and theoretical foundations

The overall objective of the studies presented in this thesis is to enhance the online resilience of online banking users. As stated earlier, to achieve this objective lessons can be learned from how end users think about threats; cases in which things have gone wrong, i.e., end users being victimised; how victims cope with incidents; and by understanding how end users can be motivated to behave cautiously when online. Although these aspects are related, they are also distinct in their own respects as will be explained later. In order to maintain overall clarity, the empirical section of this thesis is divided into two parts. Part I deals with end-users' perceptions about online banking fraud and victimization of online banking fraud, whereas Part II deals with precautionary online behaviour. As stated by Furnell and Clarke (2012, p. 984), 'In order to address the human aspects of security it is necessary to consider both the related threats […] as well as people-focused safeguards […].'

Although choosing multiple perspectives may seem extensive, it is deemed necessary. As Parsons et al. (2010, p. II) put it, how end users interact with

[29] Steering committee of the Dutch Research Program on Safety and Security of Online Banking (personal communication, July 23, 2013).

[30] Algemeen Dagblad (2013). *Diefstal via internet nekt zzp'er* [Theft over the internet disastrous for self-employed entrepreneur]. Retrieved from http://www.ad.nl/tv-en-radio/diefstal-via-internet-nekt-zzp-er~ae01f40c/

information systems and how decisions are made regarding information security is 'certainly a very dynamic and complex issue'. This means that many factors need to be taken into account; this has been done in this thesis without making the whole too broad or unfocused. The theoretical foundations and concepts that are introduced in the subsequent sections are defined and elaborated in more detail in the chapters that follow in order to avoid repetition.

1.4.1 Part I: Risk perception and online banking fraud victimization

The central themes of Part I are risk perception; behaviour leading to online banking fraud victimization; victim characteristics; and coping with victimization. Insight into these aspects is important in the fight against cybercrime.

More than 30 years ago, Johnson and Tversky (1983) wrote that society was engaged in assessing, managing and controlling risk as never before. This observation still applies and extends across all layers of society (Garland, 2003). Risk – which can be defined as 'a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself' (Beck, 1992, p. 21) – is a fundamental aspect of modern society (Beck, 1992; Jackson, Allum, & Gaskell, 2005), and the same applies to the internet. In Chapter 2, risk perceptions in relation to online banking fraud victimization are studied.

To study risk, two perspectives can broadly be taken: the *revealed preferences* approach of Starr (1969) and the *expressed preferences* approach of Fischhoff, Slovic, Lichtenstein, Read, and Combs (1978). The first approach takes a positivist perspective, a rational or deductive means to evaluate risk. The second approach takes a social constructivist perspective, which evaluates risks based on perceptions and values, and is an inductive means. It seems that in the context of cybersecurity, the first perspective is often adopted, see for example the Dutch cybersecurity assessment reports (NCSC, 2015; 2016), whereas, it is – at least in this context – more appropriate to study risk within the second approach.

The underlying reason to study (subjective) perceptions of risks regarding online banking is the focus of this thesis: the human factor. Moreover, objective reality is of limited importance because perceptions are by definition not rational (Pleysier, 2011). Also, objective reality is not pertinent for the behaviour that end users demonstrate, which corresponds to the Thomas theorem: 'If men define situations as real, they are real in their consequences' (Merton, 1968, p. 475). Thus, the perceptions that end users have of risks associated with online banking primarily determine the extent to which they will interact with it. Additionally, it will give an indication of the level of trust people have in this online service. Low levels of trust in online banking (because of crime) can be harmful to the economy and society at large. Francis Fukuyama's illustrative

quote from his 1995 book *Trust: The social virtues and the creation of prosperity* backs up this claim, 'Widespread distrust in a society […] imposes a kind of tax on all forms of economic activity, a tax that high-trust societies do not have to pay'.

Because trust seems to be an important factor in online banking, this factor is included in this thesis. Not only is it important for the initial and continued acceptance of this online service (Beldad, De Jong, & Steehouder, 2010; Yousafzai et al., 2003), it is also a necessary aspect regarding uncertainties that are attributed to financial transaction in general and online transactions more specifically (Grabner-Kräuter & Faullant, 2008). However, trust is a broad concept that needs to be narrowed down. This is quite difficult as different disciplines tend to define it differently (Beldad et al., 2010; Mayer, Davis, & Schoorman, 1995; Yousafzai et al., 2003). A further complicating factor is that other terms are used as well when referring to trust. Some prefer terms like confidence or perceived trustworthiness in the context of information systems (Cheshire, Antin, & Churchill, 2010) or reliance and dependence in terms of objects and processes (Shneiderman, 2000).

This thesis adopts the concept of trust, because this term is often applied in user studies on online banking and is limited to trust in online banking: 'a psychological state which leads to the willingness of customer to perform banking transactions on the Internet, expecting that the bank will fulfil its obligations, irrespective of customer's ability to monitor or control bank's actions' (Yousafzai et al., 2003, p. 849). This definition is based on the work of Mayer et al. (1995) and Rousseau, Sitkin, Burt, and Camerer (1998) and includes two fundamental elements that are in line with most definitions of trust: (1) it is viewed as the acceptance of being exposed to risk; and (2) it is viewed as an expectation of certain behaviour by another party. The antecedents of trust are not studied in this thesis; see for example the work of Beldad et al. (2010) on this topic.

Learning more about how victimization takes place (Chapter 3) and about victim characteristics (Chapter 4) may lead to more knowledge on how to effectively prevent online banking fraud. After all, although online banking fraud schemes contain some technical aspects, human factors play a prominent role in such schemes. Perpetrators, for example, focus on vulnerable human characteristics and use deception tactics to obtain sensitive data (Parrish Jr, Bailey, & Courtney, 2009). Thus, human factors may explain why some people fall for fraudulent schemes while others do not (Jones, Towse, & Race, 2015; Parrish Jr et al., 2009), an issue that will be dealt with in this thesis.

Whereas Chapter 3 takes a grounded approach to study the phenomena of interest, Chapter 4 builds on the theoretical frameworks of the routine activity approach and protection motivation theory. The basic premise of the routine activity approach is that victimization depends on a motivated offender, a suitable target and the absence of capable guardians in a convergence of time and space (Cohen & Felson, 1979).[31] An attempt is made to extract target suitability from victims' characteristics and (protective) behaviours. Protection motivation theory, a social cognitive model that predicts precautionary behaviour (Milne, Sheeran, & Orbell, 2000) is used as a framework to provide possible additional indicators that reflect target suitability by examining capable guardians.

The final study in Part I deals with how victims cope with phishing and malware victimization (Chapter 5) and takes coping theory as a theoretical foundation. Lazarus and Folkman (1984, p. 141) give a technical definition of coping: 'constantly changing cognitive and behavioral efforts to manage specific external and/or internal demands that are appraised as taxing or exceeding the resources of the person.' Coping can take place before, during and after events (Beaudry & Pinsonneault, 2005). In this chapter, the focus is on what takes place after the events.

Attention for the coping process is important because people (who have been victimised) should become resilient to (future) attacks on their online banking. For victims to achieve this state, they first have to recover adequately from the incident. In order to understand what victims need to recover from, attention is first paid to the effects and impact or harm that is done to the victims. Levi and Burrows (2008) address the issue that it is difficult to agree on terms that express harm. This thesis adopts a comprehensive view on harm, meaning that it addresses the effect on thoughts and feelings, measurable financial costs, response costs and secondary victimization effects instigated by the handling of the incident.

Similar to the essence of protection motivation theory – which is described in greater detail in the following section – cognitive appraisal processes are of great importance in coping theory. It is evident that individuals and groups of people differ in their reactions when confronted with comparable events. For instance, one might deny that something bad had occurred, while another may become angry or depressed when confronted with a fraudulent attack. By taking into account cognitive processes – which intervene between the negative event and the reaction – variations in interpretations and reactions of individuals to

[31] Like most studies that adopt the routine activity approach, this thesis excludes offenders (Williams, 2015).

online banking fraud victimization can be understood (Lazarus & Folkman, 1984). These authors argue that the context in which an incident has taken place is included in this interpretation, as the psychological situation is 'a product of the interplay of both environment and personal factors' (p. 23). Although this study does not explicitly address contextual factors, these are implicitly present in the stories of the victims.

1.4.2 Part II: Precautionary online behaviour

The central themes of Part II are motivations for precautionary behaviour and how that behaviour can be influenced. Precautionary behaviour is aimed at reducing the vulnerability and severity of security incidents and refers to both the adoption of security technologies and conscious care behaviour (Ng et al., 2009; Rhee et al., 2009). Note that the latter can be related to promoting protective actions or limiting risky actions.

End users that are victimised may feel the urge to protect themselves in order to prevent being victimised again in the future. It is, however, important to motivate end users to protect themselves against online threats before becoming a victim. Indeed, no one wants to be victim of online banking fraud, or crimes in general. End users can protect themselves against online banking fraud by taking precautionary measures. An important question is how such behaviour can be encouraged.

In this thesis, precautionary online behaviour is operationalised as (a) adherence to the safety rules of online banking by private end users (Chapters 6 and 7); (b) technical and personal coping measures of self-employed entrepreneurs (Chapter 8); and (c) the online information-sharing behaviour of internet users (Chapter 9). Knowledge on these issues may contribute to strengthening the most important link in the safety and security of online banking, i.e., to increase the online resilience of end users, that is, to make them better able to protect themselves against online banking fraud. As opposed to a focus on coping after online banking fraud incidents in Part I, coping theory is now applied to the situation before online banking fraud has occurred (i.e., threat anticipation and action).

The leading theoretical framework that is adopted to study precautionary online behaviour is protection motivation theory (PMT), originally developed by Rogers (1975). Later revisions of PMT resulted in a broad spectrum of factors that initiate the cognitive processes that are central to PMT (Norman, Boer, & Seydel, 2005), i.e., threat appraisal and coping appraisal. These factors are labelled as sources of information, and include environmental factors (verbal persuasion and observational learning) and intrapersonal factors (personality variables and prior experience) (Floyd, Prentice-Dunn, & Rogers, 2000). Cognitive mediating

processes were also added, such as the evaluation of one's self-efficacy (Maddux & Rogers, 1983).

Another theory that plays a role in this thesis regarding predicting precautionary behaviour is the reasoned action approach (RAA) of Fishbein and Ajzen (2010). This model is an extension of the earlier theory of reasoned action (Fishbein & Ajzen, 1975) and the theory of planned behaviour (Ajzen, 1991). This approach identifies intentional behaviour to be an important predictor of actual behaviour, with the addition that one has actual behavioural control, formed by one's actual skills and abilities, and environmental factors. Intentional behaviour is predicted by attitude towards the behaviour, social norms and perceived behavioural control. Perceived behavioural control is further differentiated within this thesis in two distinct factors, namely self-efficacy (also part of PMT) and locus of control.

Whereas the first three studies in Part II focus on predicting precautionary behaviour and can in that sense be evaluated as exploratory studies, the final study focuses on how to influence that behaviour. In order to influence behaviour, an experimental study was conducted on fear appeals: 'informative communication(s) about a threat to an individual's well-being' (Milne et al., 2000, p. 107) that also contain information on efficacy and how to stimulate perceptions of it. The extent to which fear appeals raise perceived threat and increase perceived efficacy of a recommended response is tested, in this case by being vigilant about sharing personal information online to reduce vulnerability to phishing attacks.

1.5 Relevance

In this section, the practical and theoretical relevance of the studies included in this thesis are highlighted. An explanation is given for why these studies have been conducted.

1.5.1 Scientific relevance

Knowledge on information security behaviour or precautionary online behaviour of end users is far from complete. Theory based empirical research is thus scarce in this domain (Dang-Pham & Pittayachawan, 2015; Liang & Xue, 2010). Considering the end user to be the weakest link in information security (Moore & Anderson, 2011), a socio-technical or behavioural approach on security is required (Anderson & Agarwal, 2010). Anderson and Agarwal (2010, p. 613) state in this regard '[…] despite an acknowledgement of the importance of individual behavior and a recent interest in behavioral security research, there is limited understanding of what drives home computer users to behave in a secure manner online, and even less insight into how to influence their behavior.' Therefore, it is important to understand how end users behave and

what determines how this behaviour can be adjusted for the purposes of online safety.

Considering Part I of this thesis, more insight will be given into end-user perceptions of the safety and security of online banking. Research on end-user perceptions of cybercrimes in general is lacking (Garg, Huber, Camp, & Connelly, 2012) as are insights into the influence of cybercrime victimization on these perceptions (Henson, Reyns, & Fisher, 2013; Jackson et al., 2005). It is important to study end-user perceptions as these affect decision-making and consequent behaviour (Johnston & Warkentin, 2010). Thus, in order to understand how end users respond to online banking fraud attacks, it is crucial to first evaluate how they perceive online security and threats aimed at online banking. Additionally, it is important to find out what the determinants are for these perceptions. Thus, theoretical knowledge is advanced on end-user perceptions of cybercrime.

This thesis contributes to insights into online fraud victimization and predictor variables for victimization, which is also lacking (Ngo & Paternoster, 2011). Moreover, relatively speaking, much attention is paid in the literature to the technical side of online fraud (Bossler & Holt, 2009; Leukfeldt, 2017), while a more cognitive behavioural or psychological approach may make an important contribution to understanding and explaining online fraud victimization (Wiederhold, 2014). In the literature, different explanations are given on how and why end users become victims of fraudulent attacks (Hong, 2012). The value of this thesis is to find out – using data from actual cases, i.e., fraud cases that are registered by a bank – whether similar or new explanations can be found for the Dutch (online banking) context. In addition, answers to the how and why questions are needed in order to develop effective measures against online banking fraud (Downs, Holbrook, & Cranor, 2006).

Besides providing insight into the how and why, it is also interesting to find out whether certain victim characteristics may have influenced their chances of being victimised. Several studies have been conducted to find out whether the routine activity approach offers an explanation for cybercrime victimization (Bossler & Holt, 2009; Hutchings & Hayes, 2009; Ngo & Paternoster, 2011; Pratt, Holtfreter, & Reisig, 2010; Pratt et al., 2010; Van Wilsem, 2011a, 2011b). These studies show, for example, that people who are online more often, open attachments, click on pop-ups, use online banking, make purchases online and have out-dated anti-virus software are more vulnerable to online fraud victimization.

However, results regarding target suitability and absence of guardians are mixed (Bossler & Holt, 2009; Ngo & Paternoster, 2011; Williams, 2015). Leukfeldt's

(2014, 2015) empirical studies on phishing and malware – also the main cybercrimes studied in this thesis – failed to identify such characteristics, with the exception of spending more time online, and carrying out various kinds of activities which increased the risk of a malware infection. This calls for a qualitative study to provide more insight. Information gleaned during interviews is believed to be valuable for understanding actual motivations and the behaviour of individuals (Crossler et al., 2013). Therefore, a qualitative study has been conducted to find out whether explanatory factors can be identified that lead to online banking fraud victimization.

The final study in Part I concerns coping with victimization. In this study, the effects and impact of online banking fraud victimization are examined first; these are topics that are not frequently addressed in cybercrime literature. Then coping mechanisms are studied, which is important because identifying factors that contribute to crime adaption is crucial for victims' well-being (Green, Choi, & Kane, 2010).

A coping approach is also applied in Part II of this thesis, but there it is tailored to threat anticipation and action. Although this approach is adopted in various academic disciplines, such as health psychology and consumer psychology, it is quite novel in the domain of information security (Lai, Li, & Hsieh, 2012). Furthermore, relatively little is known about end-user security behaviours and how to encourage it (Anderson & Agarwal, 2010; Dang-Pham & Pittayachawan, 2015; Liang & Xue, 2010; Rhee et al., 2009). In addition, little is known about the use of technologies for financial transactions (Davinson & Sillence, 2014).

Theoretical models that encourage precautionary behaviour in an information security context are lacking and behavioural models have only recently been applied to this field of research (Davinson & Sillence, 2014). Consequently, it is still uncertain whether, and if so, which interventions are successful in promoting precautionary behaviour. By adopting protection motivation theory (PMT) and including a number of additional factors from the reasoned action approach (RAA), a theoretical basis is created to test this for online banking, which has not been done in earlier studies. In addition, an important contribution lies in how PMT is applied within the context of this study, which will be elaborated below. According to Anderson and Agarwal (2010), it is important to take into account additional, context-specific factors that may contribute to behavioural change, in this case online banking.

Most information security studies that adopted the PMT framework neglect some parts of the theory. An example of this is intrapersonal resources, such as earlier experiences (Vance, Siponen, & Pahnila, 2012). Norman et al. (2005) stress the importance of studying earlier experiences as these can be important predictors

of future behaviour. One type of earlier experiences included in this thesis is habit. Habit theory assumes that many actions are taken without thinking deeply about them, and that actions are performed because individuals are accustomed to them (Vance et al., 2012). Liang and Xue (2009) indicate that people are motivated to repeat previous actions that led to positive outcomes and avoid behaviour that led to negative outcomes.

Another type of earlier experiences that is considered within this thesis is internet experience. Earlier experiences with a website or online activities may affect end users' choices regarding safety and security issues (Chen & Bansal, 2010). A final type of earlier experiences is prior victimization. People who have been victimised tend to strongly believe that they may be victimised again in the future, whereas non-victims do not (Workman, Bommer, & Straub, 2008). This may possibly influence their processes of taking precautionary measures, which West (2008) confirms when he argues that, in general, security becomes a priority only when people have problems with it. Therefore, prior victimization is included in the research framework.

The other intrapersonal source that is associated with PMT is personality variables. Such variables include self-control, propensity to trust, propensity to take risks and personality traits such as openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism. For the sake of limiting the scope of research, these factors are not taken into account. Moreover, it is important to keep the theoretical framework as parsimonious as possible.

As previously mentioned, factors from the RAA are taken into account (Fishbein & Ajzen, 2010); these are attitude towards behaviour, social norms and perceived behaviour control – which, in this thesis, is split into self-efficacy (already present in PMT) and locus of control. The importance of attitude towards behaviour is often demonstrated in information system studies (Venkatesh, Morris, Davis, & Davis, 2003). Another contribution lies in including social norms, as this is an aspect often neglected in information systems research (Anderson & Agarwal, 2010). Locus of control is deemed important to the issue of end-user responsibility for the safety and security of online banking. End users may attribute this responsibility (to a certain extent) to themselves, or they may attribute (most) responsibility to the bank that provides this online service. Furthermore, this construct is viewed as an important aspect in the prevention of threats (Workman et al., 2008).

This thesis tests how PMT performs uniquely in relation to RAA in predicting behavioural intentions and vice versa. Furthermore, PMT and RAA are tested in an integrated fashion. These endeavours are applied to advance theoretical

knowledge and to pursue maximum effectiveness (Lippke & Ziegelmann, 2008; Sommestad, Karlzén, & Hallberg, 2015). Although these models in themselves have been extensively tested, this is not the case in the information security context. Testing this will help researchers to make informed decisions about which model to adopt in similar contexts. Moreover, the results on precautionary behavioural intentions are compared in terms of different demographic variables, i.e., gender, age and education level. This aspect is often neglected, but it is important to further differentiate the findings (Hair, Hult, Ringle, & Sarstedt, 2014).

Another factor that seems important to the online banking context is perceptions on bank reimbursement policies or perceived financial compensation if fraud occurs. Although such policies (partly) remove the risk of losing money, they do not affect how the underlying risks are perceived. Thus, perceived financial compensation is no antecedent of perceived risk (Chellappa & Pavlou, 2002), rather it is a potential surrogate for information security. When customers assume that reimbursement follows victimization by definition, they may be discouraged to take action. Conversely, if customers believe that they will have to pay for some or all of the financial damages themselves, it is expected that they will be motivated to take precautionary measures.

A final factor that is also included as a possible predictor variable that may have influence one's motivation to act cautiously online is trust in online banking. More specifically, trust is linked to the end-user's threat appraisal. Therefore, trust is adopted as an additional variable that may explain risk perception (Das & Teng, 2004). Note that this factor plays a role in both Part I and Part II of this thesis.

Another valuable contribution that this thesis offers is that it also addresses the information security behaviour of self-employed entrepreneurs. This is important since small businesses represent a vulnerable target group with potentially limited resources to fight the increasing threat of cybercrime. The importance of helping self-employed entrepreneurs in this area cannot be understated. Although research into human aspects of information security is increasing, the body of literature on this target group is limited.[32]

Finally, a contribution lies in the fact that the studies contained in this thesis are not descriptive only; one of them is also aimed at improving precautionary behaviour. Another part of PMT often neglected in information security studies is

[32] Although it is recognised that end-user behaviour in a corporate setting may be affected by organisational culture and the (security) climate in which they occur (Parsons et al., 2010), this thesis does not focus on those contextual or environmental factors per se.

environmental factors. This thesis contributes to this by conducting an experimental study of fear appeals on end-users' protection motivation. The effects of fear appeals on precautionary behaviour are not evident because some studies report that fear appeals do work (Witte & Allen, 2000), while others report that fear appeals produce counterproductive results (Peters, Ruiter, & Kok, 2013). This thesis contributes to the understanding of the effectiveness of fear appeals in precautionary online behaviour.

Although PMT is also used as the main theoretical model for this study, it is extended with the attitude variable, both as an outcome measure and a predictor for precautionary behaviour. Furthermore, the study focuses on two types of outcome, which is deemed important (Boss, Galletta, Lowry, Moody, & Polak, 2015), namely message acceptance or danger control – which refers to outcomes like attitude, intentions and behaviours – and message rejection or fear control, which refers to outcomes like avoidance, reactance and denial. The inspiration to complement the PMT framework in this matter comes from the parallel process model (Leventhal, 1970), the extended parallel process model (Witte, 1992) and the stage model of processing of fear-arousing communications (Das, De Wit, & Stroebe, 2003; De Hoog, Stroebe, & De Wit, 2005). In addition, intentional behaviour as well as (self-reported) actual behaviour are studied. Studying intentions only is considered a drawback in studies on human behaviour (Boss et al., 2015; Crossler et al., 2013).

1.5.2 Practical relevance

The study results will increase our understanding of online banking fraud victimization processes and factors contributing to victimization. It will also increase our understanding of the precautionary online behaviour of end users. When causes for victimization and motivations for safe behaviour are better understood, targeted measures can be taken to enhance end-users' online resilience. The findings thus present opportunities to increase the safety and security of online banking from an end-user perspective, for example, by applying the findings to the design of an awareness campaign for safe online banking.

Resilient end users have various characteristics. They are aware of threats aimed at online banking, try to prevent threats from manifesting in harm, and take necessary actions when confronted with a threat. If a certain threat could not have been avoided despite all actions, it is important that end users recognise or detect it as soon as possible. When a threat is quickly noticed, negative consequences may be mitigated or possibly be avoided entirely. Thus, end users must be able to identify threats, to protect themselves against these threats, to detect threats when they cannot be avoided, and to recover from harm inflicted by the threat. In other words, resilience is not only about

eliminating threats but also about managing them. Eliminating threats altogether is an illusion because there is no such thing as one hundred per cent security. Resilience goes further than self-perceptions on competence. It also deals with active engagement in a certain environment and being able to exert influence (Zimmerman, 1995).

Online resilience, especially with regard to online banking, is of crucial importance since end users are attributed with more responsibility in keeping online banking safe and secure (Anderson, 2007; Davinson & Sillence, 2014). Moreover, this study started with the presumption that mistakes made by end users are often the main cause for online banking fraud victimization, which this thesis will also prove to a certain extent. Thus, there is a practical goal in emphasising this link.

In the first place, online resilience is important to end users themselves, beyond the online banking context too. Although financial damages due to online banking fraud may be diminishing, phishing as well as malware attacks are still a relevant problem that leads to victimization, which can have serious consequences. Apart from the monetary aspect, this kind of victimization can also have a range of psychological and emotional effects, which will be demonstrated later. Furthermore, it may even lead to identity theft with all its possible consequences (Hutchings & Hayes, 2009). In addition, according to Kritzinger and Von Solms (2010) it is essential that internet users understand risks; it is important to protect information and to be aware of the consequences when things go wrong. Overestimating risks may lead to people not using certain products or services. If risks are underestimated, it could encourage people to behave carelessly (Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011).

Resilient end users also have practical value for banks. When end users are better able to protect themselves, it should lead to further minimising online banking fraud victimization. This means that a focus on detection, repression and correction could shift to prevention. In other words, there should be a shift from stopping attacks to preventing attacks. The fewer end users are victimised, the less impact this has on the trust end users have in and the image end users have of online banking. Indeed, online banking fraud not only leads to financial losses or reduced psychological wellbeing, harm is also felt in terms of losing trust in digital payment systems (CPB, 2016). According to Statistics Netherlands, 17% of Dutch internet users occasionally refused to use online banking services because they were concerned with online safety (CBS, 2015b). Furthermore, actions to undo the damage caused by fraudulent attacks are reduced, for example reimbursing the victim, blocking and unblocking bank accounts, call centre costs, et cetera. In the end, the police force can benefit

from this as well, as less capacity will be needed for investigating and solving these types of crime.

Moreover, the study results will make clear which aspects can be addressed in order to motivate end users to behave safely and securely online, and what their current perceptions are on threats and safety measures. This is important for marketing and communication specialists as well as for bank employees who are responsible for designing security systems. Uncertainty and risk are difficult to evaluate for customers. For security system designers it is important to understand how end users make decisions regarding security and how they evaluate them (West, 2008). 'The most elegant and intuitively designed interface does not improve security if users ignore warnings, choose poor settings, or unintentionally subvert corporate policies' (West, 2008, p. 34).

The financial sector at large and banks in particular have an important role to play in informing and educating customers about phishing attacks (Purkait, 2012). In the Netherlands, the financial sector takes responsibility in this regard as they tackle this issue in several awareness campaigns. In their communications, which are targeted at all online banking customers, banks advise their customers to hang up the phone when fake security topics are discussed, to click away phishing e-mails and illegitimate websites and to call the bank when they do not trust the situation they are in. Recently, they added to their communications that customers should not send their debit card by traditional mail, as perpetrators had deployed a different modus operandi to gain access to customers' bank accounts. Banks also inform their customers in their terms and conditions about behaving safely and securely when banking online and through security warnings on the online banking website or app. This research aims to contribute to these efforts.

In academic research, efforts have also been made in educating and training end users about phishing, such as the serious games PhishGuru and Anti-Phishing Phil (Kumaraguru et al., 2010). Although both efforts showed that the research participants' phishing detection skills improved, a considerable number of individuals were still left vulnerable to a phishing attack (17.5% and 31%). Moreover, the effects do not necessarily last over time. However, there is some evidence that if end users are more resilient there are fewer successful cyberattacks (Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010).

End users must understand the importance of security measures and precautionary behaviour in protecting themselves against fraudulent attacks. Security education, training and awareness (also known as SETA) are therefore important. However, despite the priorities and efforts of governments, academia

and other organisations to combat such attacks and to warn end users, victimization still takes place. Liang and Xue (2010) state that a cognitive behavioural research perspective can contribute to effective security programs. This thesis tested a possible direction in encouraging internet user to behave safely online. This study provides insight into the effects of fear appeals on limiting vulnerability to phishing attacks by being vigilant when sharing personal information online.

1.6 Contents of the thesis

This thesis continues with Part I (Chapters 2 to 5). In Chapter 2, a survey study on risk perceptions regarding online banking fraud is presented. Chapters 3 and 4 deal with how and why end users become victims of online banking fraud and what end-user characteristics increase the chance of victimization. These qualitative studies provide insight into these matters by analysing actual cases and by analysing interviews with victims. In Chapter 5, the victim interviews are analysed a second time to provide insight into how victims cope with online banking fraud victimization. Thereafter, Part II will be discussed (Chapters 6 to 9). Chapters 6 and 7 quantitatively study end-user motivations for precautionary online behaviour. In the former chapter, protection motivation theory, the reasoned action approach and a combination of the two are tested. In the latter chapter, the combined model is complemented with additional variables and is more thoroughly corroborated. In Chapter 8, protection motivation theory is used as a framework to explain the precautionary online behaviour of self-employed entrepreneurs. Whereas the focus of the previous chapters is on explaining behaviour, Chapter 9 focuses on improving it. More precisely, a study is presented on improving precautionary online behaviour using fear appeals.[33] Finally, the research questions will be answered in Chapter 10. Furthermore, all the contents will be discussed in a comprehensive manner, overall limitations will be addressed, and theoretical and practical implications will be elaborated.

[33] Note that Chapters 2 to 9 are a collection of previously published papers, with two having the status of 'submitted' (Chapters 6 and 9). To do justice to the authors that have co-authored the papers, words like 'we' and 'our' have been retained. With the contents of these chapters being the same as how they were published, some adjustments were made. These concern the consistent use of British English, the use of the APA guidelines, numbering and naming of headings, referrals and the integration of tables (that were otherwise published in [online] appendixes). One exception, however, is Chapter 4, where context was additionally provided to the quotations. Also note that Chapter 2 is a translation of a paper published in a Dutch journal.

PART I:

RISK PERCEPTION AND ONLINE BANKING FRAUD VICTIMIZATION

CHAPTER 2

End-user perceptions of the safety and security of online banking

Jurjen Jansen

Nicolien Kop

Wouter Stol

Published in Tijdschrift voor Veiligheid 2017, 16(1), 36–51.

2.1 Introduction

More than 90% of households in the Netherlands have access to the internet (Statline, 2016b). Internet access is a convenience that many people enjoy, for instance, for staying in touch and when doing shopping. A disadvantage of the digital revolution is that people have become more dependent on technology, and more vulnerable to security incidents too (Furnell, Bryant, & Phippen, 2007). Thus, adequate information security is an essential requirement in today's society, for instance, to ensure that sensitive information does not fall into the hands of people with malicious intent.

This study focuses on a specific online service, namely online banking. Online banking gives users access to various banking services via the internet. These services include being able to check balances and pay bills, services that are used a great deal in the Netherlands. Eighty-five per cent of the Dutch population who are sixteen years and above use these services (Eurostat, 2016). Online banking offers users convenience and flexibility when carrying out financial transactions (Davinson & Sillence, 2014).

However, online banking also has a downside. Whereas in the past, banks used to get physically robbed, criminals these days use phishing or banking malware to get their hands on users' login details and security codes, which they can then use to steal money from the corresponding bank accounts. Phishing is an attempt at scamming (Section 326 of the Dutch Criminal Code): the perpetrator tries to persuade someone to part with their information using digital means and deception (often via e-mail), in order to gain unlawful advantage by doing so. Malware is a contraction of 'malicious software' and a catch-all term for harmful software like viruses, worms, Trojan horses and spyware. Phishing and malware are the most common kinds of threats that online banking users in the Netherlands face. These two threats are central to this study.

This study specifically discusses the perceptions that users have of these threats. According to Johnson and Tversky (1983) and Slovic (1987), it is important to map perceptions that people have when it comes to security, and to understand these perceptions. Perceptions of hazards and risks affect the way people make decisions and therefore their behaviour (Johnston & Warkentin, 2010). The same applies to online banking (Cunningham, Gerlach, & Harper, 2005; Jansen & Van Schaik, 2016; Yousafzai, Pallister, & Foxall, 2003). Consequently, to understand how people react to attacks on online banking, we should investigate how they view their online security and attacks on it. For this reason, this study looks specifically at risk perception. In addition, research into risk perception facilitates the design of risk communication and mitigation technologies (Garg & Camp, 2012).

For online banking, risk perception could be interpreted as the perceived potential for loss if the service is used (Yousafzai et al., 2003). We talk of perceptions because people often rely on an intuitive opinion that they have of risk (Slovic, 1987). Risks in this sense are a social construct; people base risks on emotionally loaded value judgements and also on cognitive claims (Garland, 2003) that do not necessarily correspond with reality.

The objective of this study is to gain an understanding of the risk perception that users have about online banking fraud, and to shed light on factors that influence that perception. Based on this, the central question is: What is the nature of the risk perception that users have of online banking fraud and how is this perception formed? Only little research has been done into perceived risks of the online domain (Garg, Huber, Camp, & Connelly, 2012). This study attempts to address this shortage. In addition to this, little is known about the effect that cybercrime victimization has on the way risk perception is formed (Henson, Reyns, & Fisher, 2013; Jackson, Allum, & Gaskell, 2005). This study contributes to what we know about perceived risk of the online domain by including online banking fraud victimization as a possible explanatory variable for risk perception.

2.2 Theory

Risk perception can be studied from various approaches. Two important ones are the revealed preferences approach developed by Starr (1969) and the expressed preferences approach that Fischhoff, Slovic, Lichtenstein, Read, and Combs (1978) advocate. Slovic and Peters (2006) interpret these two approaches as 'risk as analysis' and 'risk as feelings'. The former is based on logic, reasoning and scientific deliberations, and the latter on instinctive and intuitive opinions. This means, for instance, that academics assign a different meaning to risk than laymen do (Slovic, 1987).

In our study, we use the expressed preferences approach as the basic premise because we are studying end-user perceptions. This approach takes into consideration that end users do not have all the information they need and that they cannot use the information that they have as effectively as possible. This subjective alternative also plays a fundamental role in various theoretical models (e.g., Rogers [1975]), for instance, in order to get a better understanding of behaviour in relation to information security (Johnston & Warkentin, 2010; Liang & Xue, 2010).

2.2.1 Predictors of risk perception

In common parlance, risk is defined as the possibility of loss, damage, disadvantage or destruction (Garland, 2003). In a more theoretical sense, risk

can be considered to be a measure for exposure to danger, expressed in likelihood (perceived vulnerability or probability) and the extent of the loss (perceived severity or impact) (Garland, 2003; Jackson et al., 2005; Liang & Xue, 2010).

Those who study risk perception, including Griffin, Neuwirth, Dunwoody, and Giese (2004), Slovic (1987) and Vlaev, Chater, and Stewart (2009), demonstrate that risk perception has a multi-dimensional character. In addition to perceived vulnerability and perceived severity, Griffin et al. also mention personal control and institutional trust as predictors of risk perception. According to them, personal control is a self-assessment of the degree of control over the susceptibility to damage if the risk becomes reality. Furthermore, institutional trust concerns the extent to which an individual considers other parties to be capable of ensuring that the individual will not be negatively affected by the threat in question. If the perceived control of one's own safety and the degree institutional trust are high, risk perception will be lower (Griffin et al., 2004).

From the more general 'fear of crime' literature, we learn that there is a link between risk perception and fear. For this reason, we draw from this literature to find out more about the potential effect that victimization has on risk perception. Henson et al. (2013), for instance, claim that individuals who have fallen victim to a particular offence (personal experience) suffer from higher levels of fear with respect to that offence than non-victims do. Their victimization has evidently affected their perception. In addition to personal experience, the social environment and the media may have a predictive effect on perceived risk and fear (Hale, 1996; Henson et al., 2013; Jackson et al., 2005; Johnson & Tversky, 1983). This is also referred to as 'indirect victimization' or 'vicarious experience'.

For the sake of completeness, this study also investigates the effect of demographic variables. Previous research has shown that the demographic variables of gender, age, level of education and work status have a predictive effect on risk perception (Bronfman, Cifuentes, & Gutiérrez, 2008; Savage, 1993). These variables also play a predictive role in the fear of crime literature. For instance, women, older people, the less highly educated and those on low incomes generally report higher levels of fear of crime than their counterparts (Hale, 1996), even though these groups, objectively speaking, are the least likely to fall victim to crime (Pleysier, 2011). As far as age is concerned, several studies found the opposite effect, namely that younger people are more afraid of (certain kinds of) crime (Henson et al., 2013; Jackson, 2009).

The literature also mentions other factors that apparently influence risk perception. Fischhoff et al. (1978) describe nine dimensions of risk in the psychometric paradigm. In addition to the dimensions of risk control and the severity of the consequences that we have already discussed, they identify: the voluntariness of risk, the timeliness of the impact, expert knowledge about the risk, the knowledge that lay experts have about the risk, how new the risk is, whether it affects one person/system or several people/systems, and whether it is a risk that the person has learnt to live with, or one that the person fears. Cultural aspects, attitudes, risk sensitivity and specific fears may also affect the way that people perceive risks (Sjöberg, 2000). These factors could not be included in our analyses due to the limitations of the dataset that we based our secondary analysis on. We will return to this in our discussion of the findings.

2.2.2 Implications of risk perception

An important discovery in the field of psychology that Tversky and Kahneman made in 1974 was that people use heuristics (intuitive judgements) to lend significance to uncertainties (Thaler & Sunstein, 2009). While these gut feelings may hold true in some cases, in others they lead to stubborn prejudices that have implications for risk assessment.

Research into objective and subjective opinions about threats has revealed that human thinking is subject to prejudices (Slovic, Fischhoff, & Lichtenstein, 1982). For instance, the frequency of infrequent events is often overestimated and the frequency of frequent events is often underestimated. In addition, overestimation is most likely to occur for dramatic or sensational incidents, while unspectacular incidents are mainly underestimated. Huang, Rau, Salvendy, Gao, and Zhou (2011) claim that knowledge is a key factor in the gap between perceived security and the actual security of a system. A lack of knowledge is often the reason for under- or overestimating a system's level of security.

If the perceived risk is higher or lower than the actual risk, it may have negative consequences. Overestimating the risks can lead to people not using certain products or services for no good reason. 'Not using' online banking in the Dutch context is virtually inconceivable because there are very few options available. What might happen, however, is that online banking is used less often (for instance, people may avoid using it for online purchases). If the risk is underestimated, it may encourage people to behave unsafely (Huang et al., 2011).

2.3 Method

This study involved the secondary analysis of a dataset that was used for research into motivations for precautionary online behaviour by those who use

online banking (Jansen & Van Schaik, 2016). An online survey was conducted for this in mid-2015. The survey was based on literature research and it was pre-tested both qualitatively and quantitatively. For the current study, supplementary literature research was conducted to hone the theoretical framework.

The dependent variable risk perception is central to this study. We examined the extent to which the dependent variable is affected by the following independent variables: perceived vulnerability, perceived severity, locus of control, trust in online banking, and direct and indirect experience of victimization (personal, the social environment and the media). The demographic attributes of gender, age, level of education and work status were included as control variables.

Locus of control may be internal or external. Internal locus of control means that people believe that they themselves have control of certain eventualities; while with external locus of control people attribute it to fate or they lay the responsibility elsewhere (Rotter, 1966; Workman, Bommer, & Straub, 2008), for instance, with the bank. Trust in online banking is considered to be 'a psychological state which leads to the willingness of customers to perform banking transactions on the Internet, expecting that the bank will fulfil its obligations, irrespective of customer's ability to monitor or control bank's actions' (Yousafzai et al., 2003, p. 849). Studies into the adoption of online banking have shown that the perceived level of risk decreases in line with an increase in the level of trust in online banking (Davinson & Sillence, 2014; Yousafzai, Pallister, & Foxall, 2009). Locus of control and trust in online banking are closely aligned with the constructs of personal control and institutional trust (see Section 2.2.1).

The variables are based on existing scales and were measured using three statements that the participants could answer on a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The questions about the perceived level of risk were based on Grabner-Kräuter and Faullant (2008); the questions about perceived vulnerability and perceived severity were taken from Witte (1996); the locus of control questions were based on Workman et al. (2008); and the questions about trust were taken from Yousafzai et al. (2009). To measure victimization, descriptions of phishing and malware were first given to the participants, after which they were asked about the extent to which they had heard (from their own social environment and the media) of people falling victim to these threats. Participants were then asked whether they themselves had fallen victim to these threats in the previous five years. At the end of the questionnaire, participants were asked to complete their demographic details.

2.3.1 Participants

An external online panel recruitment firm wrote to and recruited the participants. In total, 1,850 people viewed the questionnaire online. Of these, 614 viewed the questionnaire but either did not complete it or did not complete it fully. We were not able to obtain additional information about the background characteristics of these people. Thirty-six people were excluded from further participation after the first screening questions because they did not belong to the target population: 14 of them have tasked someone else with the management of their online banking; and the remaining 22 did not use online banking services.

In total, 1,200 participants completed the questionnaire in full. Of the participants, 54.8% were female and 45.2% were male. The average age of the participants was 49 years (*SD* = 14.5) and the education levels were categorised as high (52.5%), medium (32.3%) and low (15.2%). Regarding work status, the participants were either employed (53.9%), entrepreneurs/self-employed (6.9%), retired (18.8%) or had another status (20.3%), for instance, they were students or seeking employment. In total, 56.9% can be considered as belonging to the working population. This group consisted of entrepreneurs/self-employed and people who were in salaried employment for twelve hours per week or more.

Because we did not have any figures about the total population in the Netherlands that uses online banking, we compared the participants' background characteristics with those of the population in the Netherlands as a whole. It is not possible to determine exactly how representative the participants are of the population in the Netherlands that uses online banking. The figures presented are therefore indicative.

Women are somewhat over-represented in the dataset, and men are slightly under-represented ($p < .01$). The distribution of the population in the Netherlands is 50.5% female and 49.5% male (Statline, 2015).[34] In comparison with the population in the Netherlands, the age category up to 30 years is under-represented in our database ($p < .001$) (Statline, 2016a).[35] Highly educated participants are over-represented and less highly educated participants are under-represented in our dataset ($p < .001$). According to Statline (2013), the distribution of education levels in 2012 was high (28.6%), medium (40.7%)

[34] Calculation based on 2015 as the reference date, total population in the Netherlands.
[35] Calculation based on 2016 as the reference date, population aged from 20 to 80 in the Netherlands.

and low (30.7%).[36] Taken across the entire working population in the Netherlands, the percentage that belongs to the working population is 64.8% (CBS, 2015a).[37] This percentage is significantly higher than the percentage in our dataset ($p < .001$).

2.3.2 Data analysis

We used SPSS (Version 23) for the descriptive analyses. To determine the extent to which the predictive variables influence risk perception, we used path analysis (partial-least-squares path-modelling [PLS]). This analysis method is suitable for exploratory research and is designed to maximise the amount of explained variance (Hair, Hult, Ringle, & Sarstedt, 2014). The explanatory analysis was carried out using the statistical software program SmartPLS 2.0 (Ringle, Wende, & Will, 2005). We used a standard PLS bootstrap procedure (N = 5,000), as recommended by Henseler, Ringle, and Sinkovics (2009), to test the significance of the parameters in the structural model. The structural model represents the relationships between the dependent and independent variables.

In addition to the structural model, PLS provides a measurement model that we first evaluated. This gave us insight into the extent to which the data fulfilled the requirements for the analysis method that we applied. The component loadings of the individual items were sufficiently high (≥ 0.70) in the corresponding construct and significant lower than the other constructs, which provides evidence for the unidimensionality of the items (Henseler et al., (2009), see Table 2.1. The reliability of the constructs was assessed based on the composite reliability coefficient. All the constructs were sufficiently reliable (≥ 0.70): risk perception (0.88), perceived vulnerability (0.88), perceived severity (0.90), locus of control (0.84) and trust in online banking (0.89).

[36] Calculation based on 2012 as the reference date, population aged from 15 to 65 in the Netherlands.

[37] Calculation based on 2015 as the reference date (first quarter), population aged from 15 to 65 in the Netherlands.

Table 2.1: Component loadings

	PR	PV	PS	LoC	TR
PR1	**0.85**	0.60	0.32	-0.22	-0.38
PR2	**0.81**	0.67	0.22	-0.28	-0.37
PR3	**0.87**	0.61	0.31	-0.29	-0.41
PV1	0.63	**0.88**	0.18	-0.26	-0.33
PV2	0.69	**0.90**	0.23	-0.28	-0.35
PV3	0.55	**0.73**	0.21	-0.19	-0.24
PS1	0.27	0.22	**0.87**	0.08	-0.08
PS2	0.20	0.13	**0.83**	0.10	-0.03
PS3	0.37	0.26	**0.91**	0.04	-0.13
LoC1	-0.27	-0.26	0.13	**0.83**	0.40
LoC2	-0.28	-0.27	0.03	**0.81**	0.39
LoC3	-0.20	-0.17	0.02	**0.77**	0.34
TR1	-0.45	-0.35	-0.12	0.41	**0.91**
TR2	-0.29	-0.26	-0.02	0.45	**0.79**
TR3	-0.41	-0.33	-0.11	0.35	**0.85**

Note. PR: perceived risk. PV: perceived vulnerability. PS: perceived severity. LoC: locus of control. TR: trust in online banking.

Convergent validity – the degree to which items in the same construct are related (Hair et al., 2014) – was assessed based on the average variance extracted (AVE). The AVE for all the constructs, with the exception of locus of control, was higher than the limit of 0.70: risk perception (0.72), perceived vulnerability (0.71), perceived severity (0.76), locus of control (0.64) and trust in online banking (0.71). We kept locus of control in the analyses because variance in the items of locus of control could be explained to a greater rather than a lesser extent (value ≥ 0.50). Discriminant validity – the extent to which a construct differs from the other constructs (Hair et al., 2014) – was determined by analysing the square root of the AVE. The corresponding value of the result must be greater than the correlations with the other constructs (Fornell-Larcker criterion). All the values met this criterion; see Table 2.2. Additional SPSS analyses did not reveal any multicollinearity issues. This means that the predictive variables did not correlate significantly with one another.

Table 2.2: Coefficients of discriminant validity

	01	02	03	04	05
01 Risk perception	0.85				
02 Perceived vulnerability	0.75	0.84			
03 Perceived severity	0.34	0.25	0.87		
04 Locus of control	-0.31	-0.29	0.08	0.80	
05 Trust in online banking	-0.46	-0.37	-0.10	0.47	0.85

Note. Off-diagonal values are correlations. Diagonal values are square root of average extracted variances.

The independent variables for phishing and malware victimization were combined and dichotomised (0 = no, 1 = yes). The correlations between these variables and risk perception are: victimization experienced by the participant him- or herself (0.08), victimization in the social environment (-0.02) and victimization reported in the media (-0.13). The demographic attributes were coded as follows: gender (0 = female, 1 = male), age (in years), level of education (1 = low, 2 = medium, 3 = high) and work status (0 = unemployed working population, 1 = employed working population). The correlations between demographic variables and risk perception were as follows: gender (-0.09), age (-0.02), level of education (-0.14) and work status (-0.05). Given the exploratory nature of this study, we included the abovementioned variables in the analysis, despite the low correlation with the dependent variables.

2.4 Results

Before we consider the results of the path analysis, we will first discuss the perceptions that users have of the risks and security of online banking, and the extent to which they have had to deal with phishing and malware victimization.

2.4.1 Perceptions of risk and security

The responses that participants gave for statements about risk perception and the predictors of risk perception are given in Table 2.3. We see that the percentage of participants that consider online banking to be risky, and of those who think it likely that they will fall victim to online banking fraud is low. For comparison purposes, another statement was included, stating that other people have a good chance of falling victim to this kind of fraud. Of the participants, 37.6% agreed or strongly agreed with this statement, whereas 16.2% disagreed or strongly disagreed with it. Participants largely agreed or strongly agreed with the statement that online banking fraud can have a major impact. As a general rule, participants agreed or strongly agreed that they can control the security of their online banking (a high score on the locus of control scale indicates internal locus of control). Finally, participants indicated that they mainly trust the online banking system. This is reflected in the fact that more than half of the participants agreed or strongly agreed with the statements in question.

Table 2.3: Item-scores (in percentages), means and standard deviations (N = 1,200)

Construct	Items	1	2	3	4	5
Risk perception (M = 2.6, *SD* = 0.79)	I am afraid of being victimized by online banking fraud	11.1	35.7	36.3	13.9	3.0
	I believe it can rather easily happen that criminals steal money during online banking sessions	11.9	43.9	34.0	8.3	1.9
	I am afraid that others can access my online bank account without my permission	8.0	36.7	33.4	18.8	3.2
Perceived vulnerability (M = 2.7, *SD* = 0.71)	I am at risk for being victimized by online banking fraud	9.4	43.2	41.2	5.3	1.0
	It is likely that I will become victim of online banking fraud	11.8	40.6	39.2	7.0	1.4
	It is possible that I will become victim of online banking fraud	3.8	24.3	39.8	28.0	4.1
Perceived severity (M = 4.0, *SD* = 0.76)	I believe that online banking fraud is a severe problem	1.3	3.7	20.8	41.6	32.8
	I believe that online banking fraud is a serious problem	0.5	4.0	17.4	47.3	30.8
	I believe that online banking fraud is a significant problem	0.5	7.8	24.2	43.0	24.6
Locus of control (M = 4.0, *SD* = 0.72)	Keeping online banking safe is within my control	0.9	1.6	13.5	47.6	36.4
	I believe that it is within my control to protect myself against online banking fraud	1.3	4.2	17.4	44.6	32.6
	The primary responsibility for protecting me against online banking fraud belongs to me	2.3	6.9	22.3	37.2	31.3
Trust in online banking (M = 3.7, *SD* = 0.70)	I trust online banking	2.1	4.7	28.7	54.0	10.5
	I trust my bank	1.9	4.5	22.7	51.1	19.8
	I trust the internet for banking transactions	2.1	6.3	32.4	51.4	7.8

Note. 1–5: totally disagree – totally agree. M: mean. SD: standard deviation.

2.4.2 Victimization

Of the participants, 16.3% knew of someone in their own environment, such as relatives, members of the family, friends or colleagues, that had fallen victim to phishing. For malware, this percentage was 21.5%. All in all, 29.6% (N = 355) of the participants knew of someone in their environment who had fallen victim to one or both kinds of online banking fraud. More than half of the participants (69.1% for phishing and 52.1% for malware) said that they did not know of any victims in their own environment, but had heard of them via the media. In total, three quarters of the participants said that they had heard of this victimization in the media (75.6%, N = 907). Respectively 8.8% and 15.1% indicated that they did not know of anyone, nor had they ever heard or read anything about online banking fraud victimization in the media. The remaining participants, 5.8% and

11.3% respectively, indicated that they did not know whether they knew of anyone or had heard about it.

We define direct victimization as concerning participants who had fallen victim in the previous five years after they had parted with information in response to a phishing attack and/or had had a malware infection that targeted online banking in this period of time. In both cases, the victims need not necessarily have lost money. Section 51a of the Dutch Code of Criminal Procedures refers to victimization in the event of financial loss or other damage if it is the direct consequence of a criminal offence, for instance information theft and/or a successful malware infection.

In response to the question of whether they themselves had been confronted with phishing, 46.8% answered in the negative. A total of 4.1% were not sure. This means that 49.1% (N = 589) had been confronted with phishing at some point. By far the majority of these had received phishing e-mails (N = 569) at some point in time. Some of them were called by phone and asked to disclose information (N = 82) or had inadvertently ended up on a phishing website (N = 27). Of that 49.1%, 71.0% (N = 418) indicated that at least one of the phishing encounters concerned online banking. In total, 2.4% admitted that they had parted with information as a consequence of a phishing attack in the previous five years (N = 10). These ten were considered to be victims in this study. Of these, six people indicated that the attack had taken place in the previous twelve months, and three of the ten said that money had been taken out of their bank account.

In response to the question of whether they themselves had been confronted with malware in the previous five years, 57.8% answered in the negative. In total, 24.8% were not sure. The percentage of participants who had been confronted with a malware infection on a device that they used for online banking was 17.4 (N = 209). Of the reported malware infections, 9.6% targeted internet banking (N = 20). These twenty participants were considered to be victims in this study. Ten participants reported that the infection had taken place in the previous twelve months, and seven of the twenty said that money had been taken out of their bank account.

Despite the fact that a considerable portion of the participants had had to deal with threats targeting online banking, we were only able to identify ten phishing and twenty malware victims. Three of them were victims of both kinds, which gives us a total of 27 individual victims (2.3%). Victimization occurs among men and women alike, among all education levels and among all age categories.

2.4.3 Predicting risk perception

We used path analysis to evaluate the extent to which the independent variables predicted the dependent variable risk perception. The results of this analysis are given in the structural model, see Table 2.4.

Table 2.4: Test results of the structural model

Dependent variable	R^2	Predictor variables	Beta	Standard error	t^a
Risk perception	0.64	Perceived vulnerability	0.61	0.02	**26.62**
		Perceived severity	0.17	0.02	**8.49**
		Locus of control	-0.05	0.02	**2.41**
		Trust in online banking	-0.18	0.03	**7.40**
		Victimization (self)	0.03	0.02	1.87
		Victimization (environment)	-0.04	0.02	**2.25**
		Victimization (media)	-0.04	0.02	**2.09**
		Gender	-0.05	0.02	**2.44**
		Age	-0.06	0.02	**2.89**
		Level of education	-0.07	0.02	**3.90**
		Work status	-0.02	0.02	1.18

Note. The values in bold are significant ($t \geq 1.96$ [$\alpha = .05$], $t \geq 2.57$ [$\alpha = .01$]).
[a]Bootstrap, N = 5,000.

The structural model shows us that 64% of the variance for risk perception can be explained ($R^2 = .64$). The strongest predictor for risk perception is the perceived vulnerability of online banking fraud. We interpret the effect size as suggested by Cohen (1988): small (.02), moderate (.15) and large (.35). Two predictors that contribute moderately are the perceived severity of online banking fraud and the level of trust in online banking, whereby the latter reflects a negative correlation with risk perception. Internal locus of control is also characterised by a negative correlation, but is not as strong as an explanatory variable. Two marginally significant (negative) links were found for victimization. Demographic variables do little to explain variance, but gender, age and level of education are statistically significant.

2.5 Conclusion and discussion

Our study shows that online banking users do not consider online banking fraud to be a major risk. The same applies to the likelihood of falling victim to this kind of crime. Users estimate their own chances of falling victim to it to be lower than the chances that other people might. That people tend to underestimate their own risks and overestimate the risks that others face corresponds to what is known about this phenomenon in the literature (Workman et al., 2008). As opposed to this, the impact of online banking fraud is estimated to be high.

Participants have a reasonable amount of trust in online banking, and tend to think that there are not many risks associated with online banking fraud. That is

all very well, but it brings potential danger in its wake. The literature that uses 'risk as feelings' as its basic premise has shown that there is a correlation between risk perception and communicating the advantages of a (high-risk) activity (Finucane, Alhakami, Slovic, & Johnson, 2000). The greater the advantage, the lower the perception of risk and vice versa. It is therefore important for banks to strike a good balance between the convenience of their services, on the one hand, and their security, on the other hand. This applies not only to use of these services, but also to communications about these services. Indeed, underestimating risks can encourage people to behave unsafely, and that ultimately increases the risk. Hale (1996), for instance, argues that it is a good thing that people have some degree of concern when it comes to crime, so that they guard against it.

Participants had little direct experience with online banking fraud victimization. There were ten phishing and twenty malware victims; in total, there were 27 individual victims, i.e., 2.3% of the participants. These kinds of percentages come as no surprise if we compare them to figures from Statistics Netherlands (CBS, 2015b): around 6% of the population in the Netherlands had been confronted with malware involving the loss of information, and around 3% with online fraud. The difference with our research is that the figures published by Statistics Netherlands were aimed at general online issues, whereas our figures only related to online banking.

When discussing victimization issues, it is important to note that participants may not have noticed phishing and malware attacks. It is conceivable that malware may have embedded itself in the end-users' systems without them being aware of it, for instance, because virus scanners failed to pick it up. Participants may also have forgotten certain incidents because the questions related to the previous five years. Therefore, it may well be that the percentage of phishing and malware victims is in fact higher.

The structural model shows that the predictive variables in the literature are significant in terms of what was predicted. This means that if users assess the vulnerability (large effect) and the severity (moderate effect) to be significant, their perceived level of risk will be higher. It also means that if users have a great deal of trust in online banking (moderate effect) and if they think that they themselves control the security of online banking (small effect), their perceived level of risk is lower.

Victim variables hardly affect the explained variance of risk perception. Direct victimization does not have a significant predictive effect. This is contra-intuitive. That we did not find a significant correlation presumably has to do with

the 'perceived vulnarability' variable. This variable correlates significantly with risk perception, although the correlation level is acceptable according to the Fornell-Larcker criterion. If we do not take this predictor into consideration in the structural model, then we see that victimization experienced by the participants themselves does have a significant positive effect on risk perception. The impact of victimization experienced by the participants themselves therefore seems to be explained away by perceived vulnerability. This, however, does not alter the conclusion of the study, because the impact of victimization on the explained variance of risk perception remains limited in that case too.

Indirect victimization has a marginal effect, but in an unexpected way. That experience with victimization in the social environment reduces the perceived level of risk may be explained by the fact that participants hear stories from victims about how they were fully compensated for their loss. Another possibility is that they had been given an explanation about how the attack took place and, because of this, participants were better prepared. As a result, they were inclined to estimate the risk to be lower. In their research, Henson et al. (2013) also discovered a significant negative correlation between fear and indirect victimization. The possible explanation that they put forward is that victims tend to trivialise their experience, or to not take it seriously, which may affect the perceptions that participants have. The negative correlation between media reports and risk perception may be due to advertising campaigns in which users are offered a perspective for action that contributes to the security of online banking, which in turn may lead to people thinking that they are running less risk. Alternatively, people may estimate the risk to be low because the claim amounts that are told about are relatively small. Research that will explore these questions in greater depth is required to find out whether the assumptions presented above are correct.

In line with the literature, demographic variables alone add little to the explained variance of risk perception, but are statistically significant (Bronfman et al., 2008). An exception to this is work status. Women, young people and those with lower levels of education have higher levels of risk perception for online banking fraud than men, older people and those with higher levels of education. That women and those with lower levels of education score higher in this regard corresponds with what is known from the literature. The current study revealed that young people perceive the risk of online banking fraud to be higher than older people do, while generally speaking older people often report higher levels of risk perception. That said, Henson et al. (2013) conclude that age is not a consistent predictor of risk perception. It is possible that the 'perceived vulnerability' variable may affect the predictive effect of age. If we

remove this variable, it becomes apparent that age no longer plays a role as a significant predictor.

Although 64% of the variance in risk perception is explained, additional research is needed to find out which other variables influence risk perception. An option is to take the dimensions from the psychometric paradigm (Fischhoff et al., 1978) as the basic premise (see Section 2.2.1). A basis for this can be found in the work that Garg and Camp (2012) have done in which they applied the psychometric paradigm to online risks. Additional dimensions may contribute to the explained variance of risk perception. Also, variables that focus more on the human factor may contribute, for instance, risk sensitivity and risk appetite. We were not able to take these kinds of variables into consideration in this study because of the limitations in the dataset that we used to carry out the secondary analysis.

Because the risk of online banking fraud cannot be ruled out, it is important to continue to invest in the ability of online banking users to defend themselves, for instance, by informing them about the risks and the options that they have to combat these risks. Our results indicate that it would be useful when communicating with users to take perceived vulnerability into consideration, because this variable has the most impact on risk perception. This means that the objective of the communication should not be that everyone thinks that online banking is 100% safe. That may encourage or exacerbate unsafe behaviour. Instead it is important that users be made sufficiently aware of the risks they face so that they are on guard and take appropriate measures for a safe online banking experience.

CHAPTER 3

How people help fraudsters steal their money: An analysis of 600 online banking fraud cases

Jurjen Jansen

Rutger Leukfeldt

Published in Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust, 24–31.

3.1 Introduction

The goal of this chapter is to shed light on the circumstances around bank customers being victimized in phishing and malware attacks and how these attacks manifest in practice. Based on this information, we try to find evidence for new and/or existing fraud mitigation strategies to cope with threats aimed at online banking.

Phishing and malware attacks are the most common crimes regarding online banking fraud in the Netherlands (NVB, 2013). 'Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target' (Lastdrager, 2014, p. 8). In case of online banking, information refers to credentials and security codes. Fraudsters use false e-mails and fake websites portrayed as genuine sites of banks to gather information (Hong, 2012; Nhan, Kinkade, & Burns, 2009). Social engineering techniques that are used include using names of credible organizations or current events in combination with statements appealing to fear, threat, urgency or excitement, to influence people to react (Vishwanath, Herath, Chen, Wang, & Rao, 2011). Malware is an umbrella term for malicious software such as viruses, worms, Trojan horses and spyware. With this kind of software, criminals are able to steal digital data or gain control over a customer's computer and, for example, manipulate what a customer sees on his screen. When criminals have obtained the right information, they are able to steal money from customers' bank accounts.

This study contributes to literature by examining user behaviour in a distinctive way, namely by studying fraud cases that are registered by a bank. The outcomes can help professionals and scholars to advance interventions promoting safe online banking behaviour or raising awareness, which ultimately lead to a decrease of online banking fraud. As Downs, Holbrook, and Cranor (2006, p. 79) put it 'in order to develop tools that will be effective in combating these schemes, we first must know how and why people fall for them'.

We begin with a brief overview of related work in Section 3.2. In Section 3.3, we describe the data. Section 3.4 continues with the results. Customer behaviour regarding phishing and malware victimization is presented. In Section 3.5, we present our conclusions, reflect on them and formulate recommendations for fraud mitigation strategies. Furthermore, the limitations of our study and ideas for future research are discussed.

3.2 Theory

There are broadly two perspectives that are used to study topics like phishing (Vishwanath et al., 2011). The first is a computer sciences perspective focusing

on technological fixes that automate the detection of phishing e-mails or alert users (Abbasi, Zhang, Zimbra, Chen, & Nunamaker Jr, 2010; Ludl, McAllister, Kirda, & Kruegel, 2007; Wu, Miller, & Garfinkel, 2006). The second is a social sciences perspective focusing on individuals (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). Research has shown that (technical) security alone is not sufficient for safe online banking. Customers who are using these services are also an important factor (Davinson & Sillence, 2014; Hong, 2012; Liang & Xue, 2010; Ng, Kankanhalli, & Xu, 2009), or as Rhee, Kim, and Ryu (2009, p. 816) state 'The ultimate success of information security depends on appropriate information security practice behaviours by the end users'. Therefore, the behaviour of customers leading to victimization is examined.

While some researchers study elements of fraudulent messages (Chang & Chong, 2010; Jakobsson, 2007), how people process security indicators (Dhamija, Tygar, & Hearst, 2006; Tsow & Jakobsson, 2007), what strategies individuals choose to protect themselves against phishing (Downs et al., 2006) and factors concerning (susceptibility to) victimization (Bossler & Holt, 2009; Leukfeldt, 2014; Vishwanath et al., 2011), we try to find answers how and why customers fall for phishing and malware schemes by analysing fraud cases that are registered internally by banks. Thus, instead of studying predetermined constructs, we take a grounded approach and reflect on the information provided by victims. This information is registered in an incident database of a Dutch bank. By means of studying bank data, we are able to unravel the fraudulent interaction processes, which might provide evidence for fraud mitigation strategies.

3.3 Method

For this study, case analysis was used. From April 28 to June 2, 2014, we had access to an incident database in a fraud department of a bank in the Netherlands. The database contains information about phishing and malware incidents related to online banking. The bank where this study took place was cooperative, but under the condition that it remains anonymous. Therefore, we refer to 'the bank' instead of using the name of the bank and to 'security codes' instead of the exact wording of the bank. Security codes – also known as 'one time passwords' – are codes that are used to log in to the online banking website and to make electronic payments. These codes can, for example, be created by a code calculator or are sent from the bank to the mobile phone of the customer.

This study is both exploratory and descriptive. Prior to data collection, we explored what kind of data was available in the database. Based on this exploration, we developed a case study protocol and a codebook in order to

constructively gather data and for reliability purposes. Examples of topics we distinguished were: modus operandi, contents of fraudulent messages and customer behaviour leading to victimization. During the analyses, we assigned specific labels to the data in order to make narrower descriptions of the phenomena. In case of customer behaviour, for example, we labelled: clicking on a link, giving away security codes, entering personal details, et cetera. In order to test for construct validity, key informants of the bank reviewed our draft research report.

We managed to find the cases by using the search fields of the database. The keyword 'phishing' was used in order to obtain phishing cases and the keyword 'trojan' for malware cases, as these are the keywords bank employees use to register these incidents. Our investigation resulted in 300 phishing and 300 malware cases. For each type of fraud, 100 cases were randomly selected from the years 2011, 2012 and 2013. Based on the total number of cases per year, a calculation was made to determine which cases should be selected, for instance, every 20th of 2,000 cases. When the initially chosen case did not include any information or was incorrect (for example, phishing instead of malware), the following case was selected. The data from the cases were anonymized and manually copied from the incident database and pasted or transcribed in Microsoft Excel.

Although we attempted to obtain a random selection of cases, some relevant cases may have been ruled out in advance. Phishing and malware cases that were not registered by bank employees under the keywords 'phishing' and 'trojan' had no chance to be selected. Moreover, the hits were polluted; the results for phishing contained malware cases and vice versa. This means that statements cannot be made about the exact number of phishing and malware cases. Consequently, it is difficult to draw any conclusions about the possible increase or decrease in the number of fraud cases.

We obtained data about the modus operandi in half of the phishing cases and in two of five malware cases. Although standardized protocols were used for gathering information, certain bank employees described cases more thoroughly or were more incisive in tracing the problem than others. In some cases, no information was available on how the incident had occurred. This leaves the question how the employee did know how to label the incident. We believe that the employee had more details at the time, but did not record it in the incident database. These are important caveats to the data collected.

Of the 600 cases we analysed, 84% (N = 504) belong to a private account and 16% (N = 95) to a corporate account. In one phishing case, it remains unknown

to what type of account it is attached. For the private accounts, it was possible to register additional details, i.e., type of account holder and year of birth. Since we have no background information on the bank's customer population, only the distributions are described. The private bank accounts were owned by men (42%), women (24%), and multiple persons (31%). In 3% of cases, the type of private account holder is unknown. The birth year of the account holder was registered in 327 cases (only for male and female account holders). The age is calculated by subtracting the year of birth from the year in which the incident took place. The age of the victims ranges from 3 to 92 years, with a mean age of 49 and a standard deviation of 17 years. In some cases, a bank account was managed by someone else, such as a parent in the case of a three-year old victim.

3.4 Results

In this section, the results are presented. Customer behaviour leading to phishing victimization is described, which is followed by a description how customers were victimized by malware attacks. The anatomy of both attack types is the same and is in line with the description of Hong (2012). The fraudulent process starts with the potential victim receiving an e-mail, a telephone call or malware. Then, the victim takes the suggested action, such as visiting a false website and entering credentials. Finally, the stolen information is monetized by the fraudster.

3.4.1 Customer behaviour and phishing victimization

150 of 300 phishing cases provided detailed information about the modus operandi. In the remaining phishing cases, no additional information about the modus operandi was available.

Main types of phishing attacks

Phishing is mainly attempted using e-mails that are distributed in the name of the bank. Customers were often directed to a phishing website that was similar to that of the bank, for example by clicking on a link in the e-mail. This was the most common form of phishing in our study (N = 100). Customers entered personal information on this website and were then led to the real website of the bank. Text box 3.1 gives an example of an individual reacting to a false e-mail. The text boxes are representative transcriptions of the main fraud types.

Text box 3.1: Private customer, male, 74 years

The account of this customer was managed by a female attendant. This woman received an e-mail which she believed was from the Abuse Desk of the bank, stating that the account of the customer was locked for protection purposes, due to illegal activities on the account, and could be unlocked via a link in the e-mail. In case of non-compliance, the bank would be obliged to restrict online banking functionality. The woman clicked on the link and filled out various details, including a security code, because she was under the impression that it was some sort of verification. A day later, the woman noticed that a fraudulent transfer of 2,000 euros had been made.

In 46 cases, we know that the victim has been called by a fraudster, which (by definition) can be considered a distinctive modus operandi next to phishing. In 29 of 46 cases, it was explicitly mentioned that victims were phished before they were called. During the phone call, fraudsters often mentioned that they work for the bank and then tell a story that seems credible to the customer. Occasionally, fraudsters mentioned that the customer should not use online banking for at least two hours, for instance, due to the processing of certain operations. Text box 3.2 presents a phishing instance in which a customer is called by a fictional bank employee.

Text box 3.2: Private customer, joint account

The customer received a phishing e-mail stating that the bank had programmed a new web application meeting today's safety requirements in accordance with European directives. However, they claimed that they had received an error message concerning the account of the customer. This error could easily be solved by downloading the update page that was attached to the e-mail. The customer completed this procedure by opening the attachment, selecting multiple items and entering personal details, including phone number and account number. The next day, the customer was called by he thought was his bank. The fraudster wanted to go through the procedure step-by-step which the customer had carried out the day before. During this call, the fraudster obtained not only personal information of the customer, but also several security codes. The day after, the customer was called by the actual bank, which wanted to confirm a transfer of 13,500 euros.

Cooperating with phishing schemes

In 27 of 150 cases, no information was found on customer behaviour leading to phishing victimization. Although most customers explained that they responded to the instructions of fraudsters, some mentioned that they never received phishing e-mails nor entered or shared personal details or security codes (N =

28). In these cases, phishing victimization still has taken place. We do not know if these customers were truly unaware of this, if they tried to hide this, or if the phishing attempt has taken place by a different modus operandi. In the remaining 95 cases, we obtained details about the role of the customer in the fraud process. In some case descriptions, more than one detail was included. Customers shared information with fraudsters ranging from personal data (N = 55) to security codes (N = 42) and performed actions such as clicking on a link (N = 36) and actions which were stated in the phishing e-mail or given by the fraudster during a telephone conversation (N = 20).

Phishing victims trusted the messages fraudsters send to them. The messages appeared to be sent from the bank and the content seemed reliable. Furthermore, victims reported that the design of the message resembled that of their bank, for example, the bank's logo was visible and similar fonts and colours were used. The false websites, resembling those of the bank, were also perceived trustworthy by the victims.

The reasons why customers responded to a message or cooperated with a fraudster were diverse. Fraudsters used several techniques to trick customers into sharing personal information or security codes. In 68 cases, we know the topic fraudsters addressed. They often addressed topics related to the security of online banking (N = 36), topics related to the bank account (N = 16) and topics related to customer verification (N = 9). Examples include the need to change log-in codes, to verify the bank account, and to perform actions due to illegal activities that have taken place on the account. In some cases, the message was threatening or mandatory in nature, for instance by stating that the customer was obliged to perform an action. In seven cases, different topics were addressed, such as cancelling an online payment. The customer in question never ordered the particular product and therefore followed the instructions given by the fraudsters. One case appeared to be a targeted attack (i.e., spear-phishing), because the customer was asked to make changes due to a change of treasurer.

We believe that customers did not suspect that something was wrong. They were reassured by the message they read, by safety signs on a website, such as a closed padlock, or by the answers provided by the fraudster via telephone. In some cases, filling out personal information was just the first step in the phishing process. Various e-mails contained a message that the customer would be called. Some customers who were insecure about the phone call asked the fraudster questions (N = 9). A private customer, for example, asked how he or she could be sure that the bank was calling. The caller asked the customer to name a date and confirmed which transfers and payments were made on that

particular day, which made the customer trust the intentions of the caller. In another case, the caller could name the account number of the employer of a customer and answered other questions perfectly. Some customers gave away security codes because the conversation with the fraudster was perceived pleasant and trustworthy.

Several customers had a certain reference (N = 15). In five cases, the customer received a fraudulent message which was referred to in the telephone conversation with the fraudster. Another example we observed was fraudsters making use of developments in the banking industry, for instance the transition to IBAN. (As of August 1st 2014, the Netherlands has adopted the IBAN – International Bank Account Number – system for domestic payments). Such phishing messages were perceived to be genuine, because the topic gained frequent attention in the news. In two cases, customers mentioned that they were not suspecting anything because they believed they were participating in a research project on security by the bank. In one case, a private customer mentioned that he assumed that the fraudulent message referred to a security alert he had been receiving for some time on his computer. Another customer stated that he thought the message corresponded with a recent change of the online banking log-in screen.

Furthermore, we noticed that three customers were not attentive during the fraud process or did not properly process the fraudulent messages. In one case, a customer noticed afterwards that the phishing e-mail was not directed to him personally and was sent from a peculiar e-mail address. The other two cases are examples of not reading thoroughly what was stated in the message.

It also became apparent that when customers performed particular actions, initiated by phishing messages or telephone calls, they felt uncomfortable (N = 11). We observed this both during and shortly after the fraudulent activity had taken place. In one case, a fraudster reported to the customer that things were not working and terminated the connection. This left the customer with an unpleasant feeling which made him call his bank. Other customers reported that they had a suspicious feeling after the call was ended or after completing an action. In some cases, they immediately called the bank and in other cases they first checked their account balance. Additionally, we found that a conversation with one's partner or another family member made the customer question the authenticity of the conversation (N = 4).

Other reasons why customers contacted the bank include that they noticed an unfamiliar payment and/or that the amount on their account balance did not make sense (N = 20) or that they could not log in to their online bank account

and/or were unable to perform transactions (N = 7). Based on the story of the customer and the expertise of the bank, it became clear that it was a phishing attempt.

3.4.2 Customer behaviour and malware victimization

We could distil information about the modus operandi in 168 of 300 malware cases. The remaining 132 malware cases did not include additional information about the type of malware (attack) used by fraudsters.

Main types of malware attacks

Malware victimization concerns the infection of the device a customer uses for online banking. By means of the installed malware, fraudsters were able to manipulate the online banking session of a customer. Manipulation mainly refers to injecting additional input fields, for example to retrieve a telephone number or security code, and to placing fraudulent transfers or altering genuine transfers to one or more beneficiaries in the transfer list. In other cases, fraudsters were able to obtain full access to the online bank account(s) of customers. In most of the malware cases (N = 108), customers responded to a pop-up window when visiting the website of the bank (see Text box 3.3 for an example).

Text box 3.3: Private customer, male, 59 years

After the login-procedure on the bank's website, a pop-up appeared. The pop-up had the same look as the bank's website and contained a message that the PC of the customer would be checked: 'We will check your system. This may take some time' (translated from Dutch). According to the customer, this check took about 30 seconds and then he received another pop-up. The customer needed to enter a security code to confirm that the check was completed. The customer entered the code, made a few transactions and logged out. The next day, the customer logged in to his online bank account and noticed that an amount of nearly 1,500 euros was missing.

The second most common type of malware victimization (N = 16), which we observed for the first time in 2013 and only within the private customer group, was that customers needed to install a malicious app on their mobile phones. In these cases, customers also had malware on their computer. These customers received a message to install the malicious app in combination with instructions, for example by clicking on a link or by scanning a QR-code. Of these victims, four mentioned that they needed to fill out the brand and type of their phone. Additionally, six victims mentioned that after the installation of the app, they needed to enter a code on the banking website. In Text box 3.4, an example is given of a victim who had to install a malicious app.

Text box 3.4: Private customer, female, 34 years

The customer logged in to the online banking website on the laptop of her boyfriend. Within a few seconds, a request appeared to install an app on her phone called '[bank name] certificate'. This was required in order to prevent fraud. Her phone number was already partly filled in. Only the last three digits needed to be entered, which she did. Two minutes later, the customer received a message on her phone including a link to download the app. The customer complied and was directed to a screen stating that she should allow the installing of apps from unknown sources, which she accepted. Then a log-in screen appeared where she chose a username and password. Thereafter, an activation code appeared which the customer entered on the bank's website. The customer logged in to her bank account, checked her balance, and logged out. Two days later, the customer checked her balance via an online banking app and detected that an amount of 1,300 euros was reserved.

In 44 cases, it was described in general terms that customers were victimized by means of a Trojan or a virus. Sometimes a specific type of malware was registered, such as a Zeus infection. Although we have some understanding of how customers were victimized, we have no information on how the malware infection was established.

Cooperating with malware schemes

In 24 of 168 cases, no information was found on customer behaviour leading to malware victimization. Although most customers explained that they responded to the instructions on their screens, some mentioned that they did not enter or share personal details or security codes, or that they could not remember doing so (N = 25). In these cases, however, they were still victimized. We do not know if these customers were truly unaware or if they tried to obscure it. In 119 malware cases, more specific information was available about the role of the customer in the fraud process. In some case descriptions, more than one detail was included. Information customers shared with fraudsters ranges from security codes (N = 85) to personal information (N = 19). Actions customers performed ranges from installing a malicious application on a mobile phone (N = 16) to logging in to online banking from a compromised device (N = 2).

Victims generally trusted the messages fraudsters sent to them because they were formatted in the style of the bank and the content seemed reliable to them. In 105 cases, we know the topic of the fraudulent message. Fraudsters often responded to the security of online banking (N = 49). They used different excuses to trick customers into filling out personal information or security codes. Examples of security related topics include (additional) security checks,

improving or updating the security of the online banking system, and warnings, e.g., that the online banking program was not properly closed the last time it was used. The second and third most common messages were that a security code needed to be entered in order to proceed with the log-in procedure (N = 30) and to verify the customer's identity (N = 20). In six cases, another topic was addressed, such as letting a customer make a try-out wire transfer.

We believe that victims did not suspect that something was wrong, because they were under the assumption that they performed actions commissioned by their bank and were reassured by the message they read. At other times, customers made reassurances themselves, for instance by checking whether the connection with the bank's website was secured (N = 7). Some customers had some sort of reference (N = 3). A private customer reported responding to a pop-up window because at an earlier moment she had witnessed that the bank was performing maintenance on its website. Another customer assumed that there was a new form of security on the online banking website because she had received a letter from the bank about the security of online banking a week before. These customers linked both events to each other. Another example was a message that began with 'as is known from the news'.

The reasons why customers responded to a message were diverse. Frequently, customers did this because they wanted to make sure that online banking was safe and/or make use of the bank's website. The latter could only be achieved when performing the actions as stated on the screen. One customer reported that he entered a security code, because the pop-up window could not be closed before this was done. According to this customer, not being able to close the pop-up was a confirmation of the authenticity of the screen. In one case, the tone of the message was threatening to the customer; when not filling in a security code the bank account would be blocked.

We also noticed that several customers were not alert while performing transactions or checking information (N = 7). Some customers stated that they did not read well what was presented on their screen. A private customer received an instruction, after reacting to a pop-up, which stated that an amount of approximately 800 euros would be transferred. The customer was, in her own words, too distracted to process the content of the message properly and entered the code. Moreover, reasons like being in a hurry and dealing with certain life events, such as the death of a family member, played a role. A private customer wanted to know what her balance was. Because she was in a hurry, she followed the instructions on the screen and entered a security code. Half an hour later, she was called by the bank with the question if it was her intent to transfer 1,800 euros to a bank account in a foreign country.

Furthermore, we observed that customers justified abnormalities when encountering them in the online banking process (N = 6). For example, a customer wanted to make an online payment of over 600 euros. The customer received an instruction with a security code for a payment of approximately 200 euros. The customer thought that this amount was perhaps a down payment, entered the code, and a fraudulent payment was completed. Another example is a customer who entered a security code after logging in to the bank's website. Although the customer was somewhat surprised that a security code needed to be entered at that stage, he or she was also assuming that the bank was attempting to improve security.

In other cases, customers were not aware that they were doing anything wrong. Such cases include Trojans that use overlay functionality (N = 19), by which original output is covered by manipulated output. Examples of malware by which an overlay was used are fraudulent payments that were not set off against the account balance, fraudulent payments that were not visible on the payment summary screen and a combination of both. A clear example is seen in three cases in which corporate customers were under the assumption that they were transferring money to the Dutch Tax and Customs Administration, which was in fact visible on their screens, while in reality these amounts were transferred to a third party.

It also became apparent that when customers performed particular actions, due to the malware infection, they felt uncomfortable (N = 4). We observed this in the case descriptions both during and shortly after the fraudulent activity had taken place. This uncomfortable feeling by customers was motivated by an abnormality in the online banking procedure, such as entering a security code before logging in or before a payment procedure was started. Customers who experienced such feelings during the action they performed did, however, still continue the action. Because customers were struck by uncertainty (afterwards), they decided to contact their bank.

Other reasons why customers contacted the bank include that they noticed an unfamiliar payment and/or that the amount on their account balance did not make sense (N = 48) or that they could not log in to their online bank account and/or were unable to perform transactions (N = 12). Based on the story of the customer and the expertise of the bank, it became clear that it was a case of (attempted) fraud.

Once customers understood what had happened, they often realized that there had been signs that indicated something could be wrong. These customers reported that their online banking actions deviated from the normal process (N

= 17), for instance the log-in procedure took longer and security codes needed to be entered at a different stage, that unexpected output appeared on the screen during online banking sessions (N = 13), for example the screen turned vague, dark, grey, or white, and that the computer was running slow or crashed (N = 12).

3.5 Conclusion and discussion

In this section, the conclusions of this chapter are presented. We also discuss the findings and make suggestions for new and/or existing fraud mitigation strategies. First, conclusions regarding phishing are presented, which are followed by conclusions about malware attacks. Third, transcending conclusions are offered, which count for both phishing and malware. Forth, the main conclusions are addressed. Finally, we describe the limitations of this study and provide suggestions for future research.

3.5.1 Phishing victimization

Phishing victims often responded to a false e-mail, were called by a fraudster, or were tricked by a combination of these methods.

From psychological literature it is known that it cannot be expected that individuals judge messages in full detail in order to find markers for fraud; they are more likely to rely on judgmental heuristics in evaluating the content and authenticity of messages (Chang & Chong, 2010). A drawback of relying on such visual heuristics is that customers can easily be misled (Claessens, Dem, De Cock, Preneel, & Vandewalle, 2002). Luo, Zhang, Burd, and Seazzu (2012) mention that individuals might become accustomed to such characteristics when banks themselves send e-mails to their customers. The attacks we studied were thus successful in exploiting human cognitive biases (Luo et al., 2012), i.e., creating inaccurate mental models (Downs et al., 2006). We recommend banks to avoid sending e-mails to the private e-mail accounts of their customers. Such messages should rather be send to a customer's online banking environment, as is already adopted by some banks. In any case, banks should not include attachments or hyperlinks in their messages, as customers are prone to clicking on these. It can be questioned whether banks will adopt this recommendation, because of commercial purposes. Although customers could be trained in checking legitimacy aspects of e-mails, such as sender information and hyperlink destination (by mouse-over), it is in our opinion not realistic to hold customers responsible for making errors in this regard when banks continue sending such messages. Technical solutions could be of assistance as well, such as e-mail filters and blacklists (Hong, 2012; Ludl et al., 2007), but these solutions do provide certain drawbacks, e.g., false positives and usability issues.

Victims who responded to a phishing e-mail were often led to a phishing website. Several victims reported to have checked for safety signs on the website. However, this seems to be an ineffective strategy. Not only because these signs can be easily manipulated and the typical user is unable to determine the validity of certificates (Jakobsson, 2007), but also because most users ignore such signs (Dhamija et al., 2006). Individuals who have learned looking for safety indicators are likely to be victimized by fraud scams that spoof these indicators (Downs et al., 2006). Nevertheless, several websites, including those of banks, do present recommendations to customers in this regard. We think that it might be more fruitful to explore the possibilities of embedded training – within the online banking environment – as this can effectively teach individuals how to avoid phishing attacks (Jansson & Von Solms, 2013; Kumaraguru et al., 2010).

In some cases, there was direct contact between the customer and the fraudster by means of a telephone conversation. This form of contact was believed trustworthy by the victims. This is probably due to that fraudsters present themselves as reputable individuals working for the bank of the victim, i.e., the representativeness heuristic (Chang & Chong, 2010), which is known from literature gains trust (Nhan et al., 2009), or because the means of communication occurred on an independent channel (Jakobsson, 2007). Fraudsters also gained trust by answering questions some customers asked them and because they knew all kinds of personal details, as personalization creates trust (Jakobsson, 2007). This makes it difficult for customers not to trust the intentions of the fraudster. We believe that customers should be educated about these schemes in general and more specifically about the use of security codes. Customers are aware of not sharing their PIN code of their debit or credit cards. However, a great number of people have not realized yet that security codes should be kept secret as well. Furthermore, customers should learn to call back the bank when they receive a phone call about security topics.

3.5.2 Malware victimization

The two most common forms of malware victimization were that customers responded to a pop-up window and that they installed a malicious app on their mobile phones. The latter form is also supplemented with a malware infection on a computer. Malware attacks could as well be instigated by technological loopholes or have taken on the form of a key logger. This implies that malware attacks could also have taken place in other ways than we have described. However, we found no hard evidence for these suggestions in our data. Perhaps this is due to that such attacks are less visible to customers and, therefore, are unlikely to be explicitly reported.

A difference between the malware and phishing incidents is the type of contact between the customer and the fraudster. With malware, the contact was digital only, while in the phishing cases there was largely direct contact between the victim and fraudster. Furthermore, certain victims mentioned that they had no idea how they were victimized. Therefore, it is difficult to formulate recommendations for interventions that combat malware threats. This is especially the case since we have no information on which operating systems victims were running, whether anti-virus software was installed, et cetera.

It became apparent that customers occasionally had an active role concerning malware victimization. This means that the malware infection in itself was not the sole cause for victimization. Therefore, we recommend banks to make their customers not only aware of malware threats in general, but also aware of more specific fraudulent schemes which are using pop-ups and malicious apps on mobile phones. Nevertheless, other customers did not notice anything regarding the malware attack. This implies that an important role is also reserved to the fraud detection systems of banks.

3.5.3 Transcending conclusions about online banking fraud victimization

Victims responded similarly in phishing and malware cases. The messages were perceived professional and concerned a topic of interest to and believed by the customer. This implies that customers have had two indicators to avoid the fraudulent activity, namely by checking the lay-out and the content of the message. We conclude that victims responded to the fraudulent messages because they appealed to trust and authority.

Responses of customers included sharing personal data like phone numbers and security codes. The reasons why customers responded were diverse, but did not differ between phishing and malware. The reasons we encountered in both phishing and malware cases are that they were reassured, they had a certain reference, they could otherwise not make use of online banking functionality, they were not alert, and they justified abnormalities. This is consistent with the findings of Jakobsson (2007) who states that individuals judge relevance before authenticity. They are also in line with the results of Vishwanath et al. (2011) who state that the main reasons why individuals get phished are that they do not adequately process information, which is further influenced by one's media use habits. Another study has shown that individuals base their judgments on a messages narrative strength (Tsow & Jakobsson, 2007). It is also known that individuals set aside their concerns, when benefits are made explicit (Davinson & Sillence, 2014). An alternative possibility is that these customers found it difficult to grasp the specific security issue mechanisms (Dhamija et al., 2006),

and therefore complied with what they saw on their screen. Thus, the reasons for responding include both cognitive and motivational processes.

The above holds that customers should only make use of online banking when things are exactly going as expected. The smallest anomaly should be enough to warn customers to terminate their banking activities. In this regard, Vishwanath et al. (2011) mention that individuals should develop safe rituals, since they cannot be fully alert at all times. Examples include reading and responding to personal e-mail on fixed moments and using different e-mail addresses for different purposes.

In all attack types, it became apparent that customers got an uncomfortable feeling both during and shortly after the fraudulent activity. This suggests that some customers acted against their own better judgment. Prevention programs could pay attention to that customers should trust their instincts when it comes to these kinds of scams. Moreover, they should be made aware of the various trust indicators that fraudsters abuse.

We observed that fraudsters responded to both technical developments, such as using malware on mobile phones and using QR codes, and developments in the banking industry which can be addressed in fraudulent messages. The latter could be considered availability heuristic (Chang & Chong, 2010). We believe that it is important to educate customers about such developments, about new techniques that are applied by fraudsters and about the cognitive influences that are involved in the fraud (Chang & Chong, 2010).

Finally, we observed in some cases that although customers quickly alerted the bank when they saw an anomaly or discovered that money was missing, the bank could not always stop the transaction and/or retrieve (all) the money. Therefore, it could be wise for banks to consider implementing a delay in wire transfers, for example transfers above a certain amount.

3.5.4 Main conclusions

In light of the above, we conclude that the behaviour of customers in the fraudulent process entails giving away information such as security codes. They do so because they go along with a fraudulent story and because they are not sufficiently suspicious. Thus, customers often actively participate in the offences of which they become victim. Another main conclusion is that customers not always trusted the intention of the fraudster, but were mentally unable to stop the process. These customers still shared information and then understood that they did something they should not have done.

What we observe here is that, if the attempted fraud resembles or is in line with the image customers have of reality (i.e., their mental model), then the chance increases to fall victim to fraud. The challenge for banks is to create such an image of reality for online banking that no story can adjust that. This can only be achieved when the image of reality is simple and kept constant. We believe that customers are then better able to detect anomalies and will, accordingly, be less likely to cooperate when they are prompted by a new, false signal.

Online banking customers should thus be able to cope with phishing and malware attacks. Creating a stable reality is one solution that may contribute to this. Furthermore, it is essential that customers are capable of understanding the threats of online banking as well as recognizing and trying to prevent them. A fruitful area for further exploration might be the coping approach. This approach is supported by various scientific disciplines, such as health and consumer psychology, but is relatively new in the field of information systems (Lai, Li, & Hsieh, 2012). We recommend applying coping theories, such as protection motivation theory (Rogers, 1975), to study the extent to which customers protect themselves against online banking threats and what motivates them to do so. In such models, an important place is devoted to risk perceptions.

3.5.5 Limitations

The first limitation is that our study was conducted at one bank. In order to draw stronger conclusions, it would be better to perform a similar study at different banks. Each bank has, for example, its own specific customer authentication techniques and methods of providing security codes.

More data about victim characteristics and the customer population of the bank were desirable in order to draw conclusions about the kind of customers that were victimized. In addition, no data was found on characteristics of corporate customers. Hence, we do not know whether these customers typically consist of self-employed entrepreneurs and small businesses, which may have no IT-department, or larger companies with more capital and in what sector they operate.

Furthermore, the distinction between phishing and malware may be arbitrary. During conversations with fraud researchers at the bank, it became clear, for example, that a combination of phishing (social engineering) and malware (technical engineering) is becoming a more common method to commit fraud. However, we found no evidence for this statement. Future research into more recent cases might reveal this hybrid attack type.

Finally, the findings should be interpreted with some caution. In half of the phishing cases and two in five malware cases, we are reasonably confident what transpired. This means that in over fifty per cent of all cases we are not certain. This is partly because we distilled cases by means of a tool used for other purposes than scientific research. Information is only imported in the tool when the bank employee considers it to be relevant. Although we obtained information in a rather unique way, it should be stressed that the data are not complete.

3.5.6 Future research

The aim of the study was to identify the role customers play in the process of phishing and malware victimization and to find evidence for possible prevention strategies. Different research methods can be used to tackle this aim. The method we used is case analysis. Although this study presents some new insights, also new questions arise.

It became clear that victims observed the communications of fraudsters as expressions of their own bank. This is due to the design and content of a particular message. In some cases, we detected that life events caused a decrease in alertness. It is interesting to further investigate contextual factors that influence victimization, also with regard to prevention.

The question remains whether, and if so how, phishing and malware victimization can be reduced. Although banking fraud will continue to be an arms race and probably will never be solved (Hong, 2012), it is important to find ways to prevent phishing and malware victimization as much as possible. Thus, there appears to be a need to educate online banking customers about how to avoid the fraudulent schemes presented in this study. We understand that customer behaviour plays an important part. When individuals become more aware of the nature of these fraudulent schemes, they are better situated to evade becoming victims (Nhan et al., 2009).

In addition, it is interesting to investigate what measures customers take to protect themselves and why they do so. Do customers in general and more specifically victims protect themselves adequately against online banking threats and how (awareness, skills, online safety cues, security software)? It is possible that such issues affect customer behaviour and the chance to be victimized. Therefore, these as well as other factors should be investigated in future studies.

A final opportunity for future research is studying if and how online banking behaviour of victims has changed over time. Perhaps these customers have adjusted or altered their online banking strategies, as they have learned from

the incident. These insights can be used for designing interventions. Designing relevant interventions, however, will be a challenge because fraud tactics are ever-changing, see also Downs et al. (2006).

The possibilities for future research that are presented in this section can be addressed by conducting interviews with actual phishing and malware victims. Crossler et al. (2013) mention that interviews are valuable because it is an effective method to better understand the real motivations and behaviour of individuals. To understand which behaviours are most relevant, also in comparison to bank customers who were not victimized, a questionnaire is recommended. This allows to quantitatively substantiating what factors affect online banking fraud. This could also be achieved by analysing actual end-user behaviour of online banking.

CHAPTER 4

Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization

Jurjen Jansen

Rutger Leukfeldt

Published in International Journal of Cyber Criminology 2016, 10(1), 79–91.

4.1 Introduction

This chapter describes an in-depth analysis into the behaviour and characteristics of bank customers leading to victimization caused by phishing and malware attacks, the most common crimes involving online banking fraud in the Netherlands (NVB, 2013). Phishing is 'a scalable act of deception whereby impersonation is used to obtain information from a target' (Lastdrager, 2014, p. 8). Malware is the infection of a computer by malicious software, which includes viruses, worms, Trojan horses and spyware. In both cases, the aim of the fraudsters is to deceive the customer or the system used for online banking in order to obtain user credentials and/or to gain control over customers' devices. Fraudster use user credentials to access a victim's online bank account and to validate money transfers on behalf of the victim. Phishing and malware scams, however, are significant across the world and go beyond the online banking context. The Anti-Phishing Working Group reported in their Phishing Activities Trends Report of Q4 2014 that nearly 200,000 unique phishing reports were submitted to them and that an average of 255,000 new malware threats – including variants – emerged each day (APWG, 2015).

A number of recent studies try to shed light on how and why people fall victim to these crimes and others do not (Bossler & Holt, 2009; Ngo & Paternoster, 2011; Vishwanath, Herath, Chen, Wang, & Rao, 2011). Jansen and Leukfeldt (2015), for example, carried out an exploratory study into how customers become victims of online banking fraud and demonstrate that customers have a specific role in their own victimization. Customers provide fraudsters with information, such as credentials, which fraudsters can use to steal money from their bank accounts. A study into phishing victimization shows that everybody is at risk when it comes to this type of crime (Leukfeldt, 2014). Additionally, Leukfeldt (2015) claims that this also largely holds for malware victimization; merely spending more time online, carrying out various kinds of activities, increased the risk of a malware infection.

Both of Leukfeldt's studies (2014, 2015) – which are based on an online survey – conclude that in-depth studies are necessary to increase knowledge about why customers are victimized. It is not sufficiently clear if certain individuals are more prone to being at risk for online banking fraud than others, and how it can be explained. Therefore, this study qualitatively explores, by means of interviews, what factors explain online banking fraud victimization. Crossler et al. (2013) mention that the interview is a valuable method to better understand the actual motivations and behaviour of individuals.

4.2 Theory

For this study, two theoretical perspectives are in place. First, we take a routine activity approach (Cohen & Felson, 1979) to study victim characteristics and behaviours that influence victimization. This approach is also central to the studies of Leukfeldt (2014, 2015) making it possible to assess whether our qualitative study has added value to the quantitative studies in this context. The routine activity approach holds that victimization is influenced by a combination of a motivated offender, a suitable target and the absence of a capable guardian in a convergence of time and space. We study the two latter aspects of routine activity approach, namely the suitability of targets and the capability of their guardians. Guardians can, for example, be technical security measures such as anti-virus software.

Over time, elements regarding suitability have been added to the routine activity approach. Two acronyms that often emerge are CRAVED, which stands for concealable, removable, available, valuable, enjoyable and disposable and VIVA, which stands for value, inertia, visibility and accessibility. Sutton (2009) compared the two acronyms and concluded that they deal with identical attributes. Furthermore, he argues that VIVA elements relate to characteristics that attract attention, while the additional elements of CRAVED are related to characteristics that make an object attractive for criminals. As this chapter is about characteristics of victims that make them appeal to a motivated offender, we adopt the VIVA acronym.

Value means that fraudsters are interested in individuals who, for the purposes of online banking, have large sums of money in their bank account. Cybercrime studies have shown a correlation between victimization of identity theft and households with higher incomes (Anderson, 2006; Harrell & Langton, 2013). We have excluded inertia from our study because, in the context of cybercrime, it refers to the volume of data and technological specifications of computer systems (Yar, 2005). Visibility is operationalized as online activities. Cybercrime studies show that such activities, such as downloading and spending time on social media, make targets become suitable since these increase visibility (Bossler & Holt, 2009; Hutchings & Hayes, 2009; Pratt, Holtfreter, & Reisig, 2010). Lastly, accessibility refers to weaknesses in software that can be used by fraudsters to attack customers. Although these three factors do explain victimization for some cybercrimes, Leukfeldt's (2015) study did not provide evidence for this related to online banking fraud victimization. We assess this outcome by using a more in-depth methodology.

The routine activity approach is used in numerous studies (Bossler & Holt, 2009; Hutchings & Hayes, 2009; Ngo & Paternoster, 2011; Pratt et al., 2010; Reyns,

Henson, & Fisher, 2011; Van Wilsem, 2011a; 2011b). However, a critical note we need to make relates to an issue introduced by Yar (2005) who argues that it is problematic to convert the routine activity approach from real space to cyberspace. Leukfeldt and Yar (2016) show that the significant impact of the routine activity theory elements differs greatly between different types of cybercrime. Therefore, we applied the interview method in order to overcome the issue of relying too much on analytic truths that is, measuring a limited number of predetermined items.

Protection motivation theory (Rogers, 1975), henceforth PMT, is used as the second theoretical perspective. PMT is a social cognitive theory that predicts behaviour (Milne, Sheeran, & Orbell, 2000) and seems applicable to online banking (Jansen, 2015). In PMT, two cognitive processes are central: threat appraisal and coping appraisal. The first process evaluates vulnerability to and the impact of a threat. This is continued by the second process that evaluates possible strategies to cope with a threat. This evaluation is based on response efficacy, self-efficacy and response costs. Both processes influence protection motivation, i.e., the intention of taking measures to protect online banking. We assume that not taking adequate protective measures, or not having capable guardians in place, might influence victimization. To be more precise, we do not qualitatively test PMT, rather its constructs are used as possible additional indicators explaining online banking fraud victimization.

4.3 Method

We conducted 30 semi-structured interviews with online banking fraud victims. The goal was to unravel how and why they became victims of online banking fraud. The interviews took place between October 2014 and April 2015, were recorded using a digital voice recorder and lasted 52 minutes on average. Sample questions include: What is your experience with online banking? How did the phishing/malware incident unfold? Do you have any idea why you were targeted? What protective measures did you have in place to prevent phishing/malware attacks from occurring?

Participants were recruited based on a selection of 65 police reports from the northern (N = 31) and southern (N = 34) regions of the Netherlands. A liaison officer working for the Dutch police first contacted the victims by telephone to inform them about our study and ask their permission to be approached to participate in an anonymized interview. Of the northern cases, seventeen participants agreed to be interviewed, five declined the request and nine were not reached. Of the southern cases, twelve participants agreed to be interviewed, four declined the request and two were not reached. The remaining sixteen interview candidates were not contacted because we gathered sufficient

data to complete the study. One participant was recruited via a liaison officer at the Fraud Helpdesk, a national organization for answering questions and collecting reports about fraud.

We interviewed seventeen phishing and thirteen malware victims. The mean age of the participants was 59 years (*SD* = 17) and ranged from 23 to 89 years. Thirteen participants were female and seventeen were male. Participants had different levels of education; low (N = 3), medium (N = 15) and high (N = 12). Most of them can be considered to be experienced users of online banking, having used it for at least five years (N = 23) and using it on a daily or weekly basis (N = 21).

For phishing, we interviewed sixteen private customers and one corporate customer (treasurer of a foundation). Malware victims consisted of one private customer and twelve corporate customers (e.g., self-employed entrepreneurs and small and medium-sized enterprises). In two malware cases, we did not speak with the actual victim. In one case, we interviewed the partner of the victim and in the other case the supervisor of the employee who was victimized. We have, however, included the information they provided because both were closely involved in handling the incidents. We believe that their stories contribute to studying the research problem. The private and corporate bank accounts were held at different banks in the Netherlands.

The recorded interviews were first transcribed. The transcriptions were directly sorted into the conceptual categories we defined prior to the study. In order to analyse the interview data, we used QualiCoder (Version 0.5), a type of computer-assisted qualitative data analysis software. The data within the initial categories were labelled with analytical codes to separate the data into theoretical themes (Ritchie, Lewis, McNaughton-Nicholls, & Ormston, 2014). After that, we reviewed the data extracts. A short summary of the interviews is provided in Appendix II.

The results of private and corporate customers are presented together because there is no clear distinction between their stories. In nine interviews, we discussed whether corporate customers behave differently with respect to online banking when engaging in work-related banking activities as opposed to their private use of online banking services. Three participants mentioned that their private and corporate use of online banking is the same. One of them mentioned, "In both cases, you deal with money. In either case, it would be a shame when something goes wrong" (interview 19). Six participants mentioned minor differences. Differences regarding corporate use of online banking include dealing with larger amounts of money, using online banking more frequently and

using an accountancy system. One participant mentioned being less precise when verifying individual payment details in a business context, "It should be consistent with bookkeeping" (interview 21).

4.4 Results

In the following sections, we present frequencies of particular views or experiences of participants. However, we do not claim that this provides a representative image of all online banking fraud victims since that is not the objective of the current study nor is it possible using this method. Rather, enumeration provides insight into how phenomena may vary among participants.

4.4.1 Anatomy of phishing and malware attacks

The anatomy of the phishing attacks described by the participants is in line with what is known from literature (Hong, 2012; Jansen & Leukfeldt, 2015). An attack starts with a potential victim receiving an e-mail or phone call designed to deceive them. Then, the potential victim takes the suggested action, such as giving away user credentials, which is followed by the fraudster using the stolen information to obtain money.

Of the twelve participants who received a phishing e-mail as point of entry for the scam, nine were called afterwards in order to obtain additional information. The contents of the e-mails were related to security and authentication issues surrounding online banking. In total, thirteen victims were called by a fraudster, four of whom believed this to be the starting point of the scam. The content of the phone calls focused on security as well, sometimes accompanied by the caller mentioning that the recipient should check or complete a procedure that was put in motion by the recipient of the call through an e-mail response. One phishing victim was unaware of how his information was phished. The participant, however, mentioned being aware of the numerous places where people's personal information is stored, "You have to leave your personal data everywhere" (interview 7). In addition, phishing victims often reported that the fraudulent story was perceived to be trustworthy and/or that they just were not alert enough to counter the scam.

Malware attacks take place using a similar three-stage approach, except that no direct interaction between the victim and fraudster was required. Interestingly, victims themselves were unable to reconstruct the fraud process. Six victims reported not having noticed anything when the attack was carried out. The online banking process proceeded in the way they were accustomed to. A participant stated, "There was nothing out of the ordinary. Nothing in particular which makes you think 'Huh?' afterwards" (interview 28).

Seven malware victims reported having observed an anomaly, of whom four mentioned having seen a glitch on their screen. The remaining victims indicated that the browser stopped operating, that the payment instruction disappeared and that there were problems logging in. One of these victims indicated that the anomaly occurred "quite some time" before the actual incident took place. The participants who observed an anomaly did not, however, relate these events to a malware attack. One participant stated, "It is associated with the inscrutable ways of the internet. […] It is science fiction to me" (interview 25).

We are able to make the claim about the anatomy; however, since the malware attacks were part of an investigation completed by the Dutch police. The Dutch police completed an investigation of a series of malware attacks in which infected websites were used to automatically install malware on the customers' device when visiting these websites (Leukfeldt, Kleemans, & Stol, 2017). When the customer transferred money online using the compromised device, the largest transfer was modified. The amount was split into two, whereby one amount was sent to the original recipient and one amount to the bank account of a money mule, a person responsible for transferring illegally acquired money to fraudsters. The customer approved the transaction because the fraudulent modification was not visible on screen. Moreover, the fraudulent transfer was hidden in the payment summary screen. It could only be observed when logging on to the online bank account with a device that was not infected with malware.

4.4.2 Suitability factors

Suitability factors from the routine activity approach do not seem to have any influence on victimization. Hence, the majority of victims think that the fraudster selected them randomly. A malware victim added that thinking this way is possibly for the best, "Otherwise you might believe that someone is watching over your shoulder all the time" (interview 30). A phishing victim mentioned that she had the feeling not being chosen for who she is, but because she belongs, "to a club of fools who have clicked on a link" (interview 6).

Most victims do not relate value to victimization. A phishing victim said, "I do not consider myself to be a perfect victim. There are people with much higher amounts of money in their bank accounts that it would have been better to pick" (interview 3). However, one phishing victim and three malware victims think that the value criterion might be related to victimization. The phishing victim may be targeted because of where she lives, i.e., suburb and type of house. The malware victims considered value to be a possibility, since their businesses deal with large cash flows.

We could not directly find any evidence for the visibility criterion being a risk factor. One malware victim opted that he might have accessed an unsecure website. Two phishing victims mentioned that they never logged out of their online banking sessions, but instead clicked away the window. However, they were not certain whether this had anything to do with their victimization.

During the time of the incident, all participants were using a desktop computer or laptop for their online banking activities. Except for two Apple users, all participants used some version of Microsoft Windows. Most participants were not aware of any weaknesses in their technical infrastructure that may have led to victimization. Therefore, we cannot conclude that the accessibility criterion is of importance. Two phishing victims stated, however, that this could be a possibility. One participant mentioned that his security subscription needed to be extended and one suspected that his computer had been hacked. Two malware victims also linked a security flaw to victimization. One of these victims explained that one of the business computers was not equipped with anti-virus software. The other mentioned that it could be associated with a Java update he continuously declined to install. He stated, "A message from Java constantly appeared on my screen wanting me to install an update. I have never clicked on this message because Java sounded like something illegal" (interview 29). However, all four participants were not sure if the security issue they mentioned is the (true) cause of victimization.

Some participants came up with other reasons for why they might be considered a suitable target. Several phishing victims indicated that their (older) age might be a possible explanatory factor. Additionally, two phishing victims pointed out that they became suitable targets after the incident had occurred. Both had the idea that they were in a 'victim database', because at a later date, they became scam targets again. One of them said, "Maybe I am on a list of interesting addresses where there is something to be had" (interview 8).

We asked participants if they thought that a similar incident would happen again in the future in order to assess whether they considered themselves to be suitable targets now they have been victimized. Five phishing victims were adamant that it would never happen again. A participant stated, "I have learned the hard way" (interview 3). The other twelve mentioned hoping or expecting that it would never happen again. Some of these participants indicated, however, that there is always a possibility.

Malware victims responded similarly. Nine participants indicated that the chances of being victimized again are slim, but do exist. A participant replied, "It is the same as winning a lottery. There is a small chance that it will happen

again, but it is possible" (interview 19). The remaining four participants were not able to give an explicit answer. One participant blamed the obscureness of the incident for this. The others stated that if it can happen once, it can happen again, "It is a fifty-fifty chance" (interviews 21 and 26).

4.4.3 Capable guardians and protective factors

Because we did not find strong support for the suitability factors explaining victimization, we will now examine the extent to which capable guardians were in place. In this study, we define 'capable guardians' as the precautionary behaviour of participants regarding the safety and security of online banking. Where appropriate, results regarding capable guardians are supplemented by statements from PMT.

Before asking participants what protective measures they took, we first asked to what extent they were aware of the threat that they were victimized by prior to the incident. Nine participants indicated that they were not aware of phishing prior to the incident, or stated that they were unfamiliar with the modus operandi used to scam them. A phishing victim indicated that he was, "not in a position to know there could be something wrong" (interview 5) because he believed that his bank did not inform him about the threat. Five participants reported that they were aware of the existence of phishing. However, four of them also mentioned not knowing how phishing schemes manifest in practice. In the case of malware, five victims knew they could be victimized in such a fashion, although some were under the assumption that it would not happen to them. One participant mentioned, "The same is true for burglaries; you always think it will happen to someone else" (interview 24). Furthermore, six malware participants indicated not having heard of the threat they fell victim to. This topic was not discussed in the interview sessions with the remaining four participants.

We went on to ask participants how they protect themselves against threats aimed at online banking. We did so using an open-ended question first and second by letting participants fill out a list with protective measures. In general, most participants take precautions to keep online banking safe and secure. Protective measures that were mentioned most are: having good security on the device for online banking (N = 21), such as anti-virus software and the latest updates, checking the money transfer details before finalizing the transfer (N = 8), deleting suspicious e-mails or e-mails from unknown sources (N = 6), and checking whether the internet connection with the bank's website is secure (N = 5), for example by checking for https and a closed padlock. On the open-ended question, three participants indicated that they did not take any measures. A phishing victim said, "When I am using online banking services, I do not

immediately think about crime. I have no idea how I should protect myself against it" (interview 14).

After answering the open-ended question, participants could score their use of protective measures that we presented to them with 'yes', 'no' and 'do not know'. The measures we included were based on uniform safety rules for online banking, which are defined in the general terms and conditions of all banks in the Netherlands. These rules and subsequent responses are as follows: (a) keep you security codes secret (N = 29); (b) make sure your debit card is not used by other persons (N = 26); (c) secure the devices you use for online banking properly (N = 29); (d) check your bank account information at least every two weeks (N = 29); and (e) report incidents directly to your bank (N = 30). Although most participants indicated that they comply with the rules set by banks, most phishing victims admitted that they had been negligent once with respect to sharing security codes.

The participants were also asked why they take protective measures. Twelve participants indicated that the measures they take effectively assist in protecting them against fraud or that they hope that they do so. A malware victim stated, "I think I am maximally protected. However, there is always a risk. There is no such thing as one hundred per cent security" (interview 25). A phishing victim added, "If criminals really want something, they will probably achieve their goal. However, you should not open the door for them. I believe that I have locked the front and back doors" (interview 10). Participants also mentioned that they like to act according to the rules (N = 3), and to take the bank's terms and conditions into account so that they can get reimbursed (N = 2). Other participants did not have a clue whether the measures are effective in protecting them against online banking fraud, often because they do not know how security works. One phishing victim questioned the efficacy of protective measures, "In some instances, only one password is needed. The security is much too limited" (interview 6).

Another means to gain insight into participants' perceptions on response efficacy is to ask them if they could have prevented the incident. Five phishing victims thought that the incident could not have been prevented. One participant indicated, for example, that he took the same actions and measures before, during and after the incident. Another participant mentioned, "There are always moments when you just are not alert and that is when something can happen. This is not exclusive to online banking, it is true for a lot of other things" (interview 5).

Other phishing victims mentioned that the incident may have been prevented if they had been more alert when reading the phishing e-mail, if they had not performed the actions fraudsters asked them to, if they had listened to their instincts, if they had been aware that banks do not conduct such procedures via e-mail and if they had been aware of the level of sophistication of criminal schemes. In addition, a participant indicated that it is a difficult issue, "People are insecure, vulnerable, do not know exactly what the procedures are. When a message appears about IBAN [International Bank Account Number, which had just been introduced for domestic payments in the Netherlands], for example, things can easily go wrong" (interview 17).

Because it was unclear to most malware victims how the incident had happened, they were virtually unanimous that they did not know whether the incident could have been avoided (N = 9). Additionally, participants reported not having received any feedback from the police or their bank on how the incident unfolded. Two malware victims mentioned that installing a (better) virus scanner might have prevented the incident. Another participant mentioned that installing software updates might have made a difference, and yet another one stated that she may have been able to prevent the incident if she had checked whether the internet connection between her device and the bank was secure.

Eight participants experienced response costs when taking protective measures due to lack of knowledge and/or low self-efficacy when taking precautionary measures. Some mentioned that security is just too complex for them. Two illustrations of this given by phishing victims, "Someone needs to tell me exactly what to do, for example, where to click for software updates. I do not know much about computers, which makes it difficult. You are already down 0-1" (interview 1). And, "I wrote down everything on paper in order to arrange security. This is due to my age: one day you know it, the next you do not. It does not stick" (interview 15).

It is noteworthy that sixteen participants indicated that they had security assistance available or that they completely outsourced security, for example, to a family member or a security company. These participants do so because they believe that they have no knowledge or not enough about security-related issues, or because they lack the necessary skills. Outsourcing security is a means to overcome the barriers or response costs they experienced. Consequently, these participants completely trust that their security is well organized and so they feel safe. Two illustrations by malware victims, "I do not know what is done in order to secure my PC, but I am confident that it is good" (interview 23). And, "I imagine I am safe because I use a corporate security package provided by [provider]. I trust it completely" (interview 20). Three

participants consider protective measures a hassle, annoying or irritating. However, half of the participants claim to experience no response costs that hinder the usage of protective measures; it is part of their routine. A malware victim added, "You need to be alert, like in traffic. Then you also have to pay attention to red lights and putout your hand when you turn" (interview 29). Another malware victim stated that he is willing to adopt additional measures if necessary, "I am not bothered by it. I prefer to make a little more effort knowing it is safe" (interview 27).

In sum, capable guardians are in place in most cases, with the exception of four instances as reported in the suitability factors section. However, some participants mentioned difficulties with regard to the PMT variables of response efficacy, self-efficacy and response costs.

4.5 Conclusion and discussion

The current application of the routine activity approach is not adequate for distinguishing characteristics and behaviours of participants that explain why they have been contacted and/or have become victims of online banking fraud. This is atypical since most cybercrime studies paint a different picture (Anderson, 2006; Bossler & Holt, 2009; Pratt et al., 2010). However, it is in line with the results of Leukfeldt (2015). Our study concurs with his statement that it seems that everyone is at risk.

The above holds that for online banking fraud: there is simply no such a thing as a suitable target. Becoming a victim appears to be simply a coincidence in this regard, a contextual phenomenon. Victimization seems to occur because fraudsters continually adjust their modus operandi according to recent events, because they gain the trust of customers or because customers simply do not pay sufficient attention. Ngo and Paternoster (2011) claim that the routine activity approach is perhaps not the best framework for studying online threat victimization at the individual level. If we challenge this conclusion, the question then is what does make these people suitable targets? Future research could make use of different research approaches or theoretical perspectives. Studying customers' actual computer and internet behaviour, for example by analysing log files, might provide evidence for what makes them suitable targets or increases their chances of becoming fraud victims. Another possibility is to use other predictor variables in quantitative studies, for example personality factors from the Big Five Inventory.

For phishing, additional possibilities for future research might involve studying in which databases or on which social network sites victims' e-mail addresses are stored. Perhaps phishing victims were targeted because fraudsters obtained

personal information by buying e-mail addresses used for spam mailings or by hacking certain databases that are poorly protected. If this is the case, updating the security of databases could provide a barrier to stop fraudsters from obtaining these details. After all, this is how the crime script for phishing often starts. Another possibility for preventing phishing e-mails from appearing in people's inboxes includes technical solutions, like e-mail filters. However, accuracy and usability are challenges for these (Hong, 2012).

We do know, based on police intelligence, that most devices of malware victims were automatically contaminated with malware when visiting ordinary websites with outdated security. This raises the question of whether customers are the right unit of analyses or the right target group for interventions to counter malware victimization. Maybe we should target website owners and hosting companies in our efforts to reduce malware victimization.

Regarding protective measures, we found that malware victims generally take adequate measures to protect the security of their technical infrastructure. Our study found no concrete evidence that malware victims were grossly negligent about security, except for two participants: one who had outdated software and one who had no anti-virus software. Therefore, it is not possible to provide recommendations for improving security on the customer side – apart from having basic security software installed (Choi, 2008) and making sure all software packages are up to date. This backs the recommendation we presented above about debating the issue of which actors should be addressed in combating malware attacks. Having said that, in this study we rely on self-reports. It might be interesting for future research to study the actual devices of customers – including those who have been victimized – to establish how they are secured.

Phishing victims were negligent because they gave security codes to fraudsters. We believe that awareness about this threat can be raised further. In addition, online banking processes should be more transparent, e.g., customers need to know what security codes entail and what happens when they fall into the wrong hands. Although a third of the participants were aware of threats, they often did not know how these threats manifest in practice. We believe that if customers are more aware of threats, they will recognize them more easily and take actions accordingly. Experimental research could provide evidence for this suggestion. Furthermore, banks and police could play a role here, for example, by providing victims with feedback on how the attack unfolded. If victims do not understand what had happened, it is difficult for them to prevent bad things from happening again.

What also became clear is that participants were unable to properly assess the effectiveness of measures to mitigate threats. Although it may be difficult to prove a measure's efficacy, it is important to not only communicate to the customer what to do and how to do it, but also what a certain measure aims to address. Hence, PMT posits that response efficacy is an important predictor for precautionary behaviour. Because security is a difficult and obscure subject for many participants, communication about this subject must be expressed as simply as possible. When customers understand the need for protective measures and gain more insight into the underlying principles, we expect that they will be more willing to apply these measures.

While most participants perceived no response costs or barriers to taking measures, we noticed that a number of participants found it difficult to do so, often because of a lack of knowledge and self-efficacy or skills. Therefore, it is important to train customers how to apply security measures. Although some participants mentioned having outsourced security, they are still the ones that perform transactions and money transfers. Furthermore, training is important since customers are attributed with more responsibility regarding safety and security of online banking (Anderson, 2007; Davinson & Sillence, 2014). This is illustrated by the fact that some of the phishing victims were not reimbursed by their bank. This raises the question of whether customers can be held responsible when something goes wrong if they are not properly taught how to apply protective measures.

The challenge lies in what is the most effective way to train customers. It would seem obvious to offer courses on safe online banking. In the Netherlands, we note that various banks and special interest groups already offer such courses. Moreover, a special website has been set up to warn customers about online threats and to tell them how to deal with these threats (www.veiligbankieren.nl). Banks could also consider letting their customers take a test in order to see whether they are capable of using online banking safely. However, this recommendation is probably not realistic since it is more cost-effective for banks to offer online banking instead of traditional banking methods. Besides, banks would not be keen to lose customers to other banks that do not implement tests. Therefore, a more effective way would be to explore using embedded training (Jansson & Von Solms, 2013; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010) that is integrated within the online banking environments. This way customers receive relevant information in a relevant place and on a relevant time, namely when they are actually using online banking – without interrupting the payment process too much needless to say. It is claimed that learning is more meaningful when rooted in the social and physical context in which it is used (Brown, Collins, & Duguid, 1989). It is also

important to periodically repeat this kind of training. Research on cardiopulmonary resuscitation (CPR) skills retention, for example, shows that not only participants' skills, but also their knowledge, already decrease after a two-month interval (Einspruch, Lynch, Aufderheide, Nichol, & Becker, 2007).

Although a smooth online banking experience is critical, it is essential to identify the best solution for educating and training customers. Future research may seek evidence for this suggestion. Furthermore, it is important to answer the question of whose responsibility it is. Is it a duty for banks in particular because they offer online banking services? Or is it a problem for society – one that falls within the scope of online safety and security in general – and one that the government should be dealing with?

CHAPTER 5

Coping with cybercrime victimization: An exploratory study into impact and change

Jurjen Jansen

Rutger Leukfeldt

Accepted for publication in Journal of Qualitative Criminal Justice & Criminology.

5.1 Introduction

The advances of technology provide opportunities for individuals, such as business and leisure activities, but they also offers opportunities for criminals to commit crime (Bossler & Holt, 2009; Van Wilsem, 2011b). In 2015, 5% of Dutch citizens aged 15 and over were victims of hacking, 4% of marketplace fraud and 1% of identity fraud (CBS, 2016b). Furthermore, the Crime Survey for England and Wales reports 3.6 million fraud incidents in the year prior to the study. Of these, 1.9 million were cyber-related. Additionally, about 2.0 million computer misuse incidents were reported, including malware and unauthorized access to personal information (ONS, 2016). Cybercrime therefore poses serious risks to society. Besides financial damages, the effects of cybercrime may lead to reputational damage and loss of goodwill and trust.

Because a substantial number of people have to deal with these types of crime, it is important to gain insight into their effects and impact on victims. However, victim perspectives on cybercrime are an underexposed topic in the literature. In addition, we need to understand whether victims adequately recover from or effectively cope with cybercrime incidents. Green, Choi, and Kane (2010) stress that a better understanding of factors related to adaption after a crime event is crucial, primarily for victims' well-being. We contribute to this understanding for a particular type of cybercrime, namely online banking fraud.

This chapter deals with online banking fraud victimization and how victims recover from it. More specifically, we study the effects – financial, psychological, emotional and secondary victimization – and impact of phishing and malware attacks on online banking customers, two common fraudulent schemes affecting online banking in the Netherlands (Jansen & Leukfeldt, 2016). Phishing is the process that uses deception, i.e., impersonation, to retrieve personal information (Lastdrager, 2014). Phishing often starts with a deceptive e-mail, but fake websites and fraudulent phone calls are also used to intercept user credentials. Malware is defined as malicious software designed to infect a device, including viruses, worms, Trojan horses and spyware. In this case, the malware targets online banking. Although malware can be considered a type of technical engineering, in some cases human action is necessary for such an attack to succeed, for example, by opening an infected attachment in an e-mail.

Research that considers online and offline fraud and the psychological impact on its victims is scarce (Button, Nicholls, Kerr, & Owen, 2014b; Schoepfer & Piquero, 2009; Whitty & Buchanan, 2016). When online fraud is studied, the focus is often on prevalence, financial impact and victim characteristics (Kunst & Van Dijk, 2009). Moreover, there is little research available that involves

speaking with online fraud victims about their experiences (Cross, Richards, & Smith, 2016).

Button, Lewis, and Tapley (2014a) argue that the public perception of (online) fraud is often that of a victimless or low-impact crime, instigated for example by credit card fraud, in which victims tend to be financially compensated for their losses, or fraud committed against larger companies who have adequate resources to compensate for the damages. However, they exposed this as a myth by showing that some of the fraud victims that they interviewed and surveyed reported devastating impacts. The fraud scams that they investigated include identity fraud, boiler room fraud, investment fraud and lottery fraud. We contribute to literature by studying the consequences of and recovery from online banking fraud victimization.

We believe that insight into cognitive and behavioural coping responses that fraud victims use might present opportunities for online fraud prevention. Extensive research on these aspects is currently lacking in the cybercrime domain. We take a critical (victimology) angle to broaden the scope of analysis to include a consideration of harm rather than crime, and social justice rather than criminal justice (McLaughlin & Muncie, 2005). Whereas criminal law is about doing justice, victims are interested in coping with injustice or the harm that is done to them.

The remainder of this chapter is structured as follows. In Section 5.2, the theoretical background is outlined. We describe what is known in the literature about the effects and impact of crime and coping strategies related to victimization. Section 5.3 covers the methodology adopted in the current study and the results are presented in Section 5.4. The limitations and discussion are the central themes of Section 5.5. This section ends with some concluding remarks. In sum, our study tries to answer the following research questions:

RQ1: What are the financial, psychological and emotional effects of online banking fraud victimization?

RQ2: What are the secondary victimization effects of online banking fraud victimization?

RQ3: What impact does online banking fraud have on its victims?

RQ4: What are the cognitive and behavioural coping responses to online banking fraud victimization?

5.2 Theory

The background literature provides theoretical insight into the effects and impact of crimes and coping strategies to deal with the effects and impact of crimes. This information will be used to reflect on our findings. Because the topic of interest belongs to a small field of work, the literature review was broadened to more general crime and victimization studies.

5.2.1 Effects and impact of victimization

Dignan (2005) describes victimization as a highly complex process as it is made up of at least three different elements, two of which are discussed at the end of this section. The first element that he describes is the interaction between the victim and the offender, and the effects from that interaction or from the offence itself. Crime in general can have several possible effects on victims. The effects can be divided into the following categories: physical effects, financial effects (both direct and indirect), psychological and emotional effects (both short term and long term) and effects on social relationships (Dignan, 2005; Lamet & Wittebrood, 2009; Shapland & Hall, 2007) and are also applicable to online fraud victimization (Button et al., 2014a; Cross et al., 2016). Furthermore, the effects can be felt by the social environment of the victim (indirect victimization), such as family, friends and colleagues (Shapland & Hall, 2007).

A wide range of possible effects of crime victimization – both online and offline – are reported in the literature. Such effects include distress, irritation, anxiety, concentration problems, sleeping trouble, lowered self-esteem, posttraumatic stress disorder and losing trust, for example, in online commerce (Cross et al., 2016; DeValve, 2005; Kirlappos & Sasse, 2012; Sharp, Shreve-Neiger, Fremouw, Kane, & Hutton, 2003). Additionally, victims lose the perception that they are invulnerable to victimization (Frieze, Hymer, & Greenberg, 1987). It is, however, difficult to accurately describe the precise effects of certain types of crime as they can be similar to one another (Shapland & Hall, 2007). Schoepfer and Piquero (2009), for example, point out that victims of fraud – which can be considered as a type of non-violent financial crime – experience similar effects to those felt by victims of violent street crimes. Thus, fraud crimes may also have serious consequences for victims.

Dignan (2005) makes an important distinction between effects and impact. According to him, impact relates to the perceived intensity of the effects plus their duration from a victim's (subjective) viewpoint. The precise effects and impact of victimization may differ from crime to crime, but can also differ for the same crimes, prompted by individual characteristics, including age, gender and income (Button, et al., 2014a; Gale & Coupe, 2005; Lamet & Wittebrood, 2009). Women, for example, often experience more or more severe psychological

consequences than men, at least for offline financial crimes (Gale & Coupe, 2005; Lamet & Wittebrood, 2009). Shapland and Hall (2007) also mention that domestic circumstances and certain life events can have an influence on how the effects of victimization are perceived. They conclude that it is 'extremely difficult to predict which individual victim will suffer which effects to what extent' (p. 179).

Green et al. (2010) argue that victims make adjustments to the effects of crime on a continuous basis. Frieze et al. (1987) distinguish between immediate, short-term and long-term reactions. According to them, the first stage lasts from hours to days and reactions typically include numbness, disorientation, denial, disbelief and helplessness. The second stage lasts from three to eight months and includes fluctuations in feelings, such as from fear to anger, from sadness to elation and from self-pity to guilt. In the last stage, the victims resolve the trauma they have experienced by adopting successful coping strategies. However, Frieze et al. (1987) also argue that long-term effects can be problematic for the victim's well-being, for instance, leading to depression, fear, guilt, low self-esteem and relationship difficulties, which has also been demonstrated in more recent studies (Denkers & Winkel, 1998; Hanslmaier, 2013). A study on white-collar crime victims by Shover, Fox, and Mills (1994) reports, for instance, that victims suffered from psychological and financial harm even years after the incident. For online fraud victimization, anecdotal evidence is provided by a study of Cross et al. (2016) that reports long-term emotional effects of some of the victims they interviewed.

The second and third elements Dignan (2005) identifies are victims' reactions to the offence, and interactions of victims with other parties as a consequence of the offence. The former relates to changes in self-perception, attitudes and behavioural responses; these changes are examined in greater detail in the next section. Within the current context, the latter deals with organizations such as banks and criminal justice agencies. Any negative impacts resulting from these interactions can be labelled as secondary victimization. These include not being treated properly when reporting the incident, inappropriate disclosure of status information, careless handling of sensitive information and poor functioning of criminal justice (Kunst & Van Dijk, 2009). Secondary victimization is important to consider, as it can worsen the harm felt by victims (Cross et al., 2016) and hinder the victims' recovery from crime (Wemmers, 2013).

5.2.2 Coping with victimization

After an individual has been victimized and experienced some of the effects as explained in the previous section, he or she has to invest effort to overcome the situation. For this study, we use the coping approach as a framework to describe

these efforts. Lazarus and Folkman (1984, p. 141) define coping as 'constantly changing cognitive and behavioural efforts to manage specific external and/or internal demands that are appraised as taxing or exceeding the resources of the person'. In other words, coping is a dynamic process of dealing with situations in which an individual is confronted with fear, stress or threat. In the current context, we define coping as cognitive and behavioural responses against online banking fraud and its impact, resulting in psychosocial adaptation to the stressful event. How stressful an event is depends on an individual's cognitive appraisal.

The coping process starts after two appraisal processes, which Lazarus and Folkman, (1984) refer to as primary appraisal and secondary appraisal. In short, appraisal processes comprise evaluations of the significance of what is happening in relation to one's well-being. These evaluations are affected by personal and situational factors and are often subjective in nature, because individuals do not always have access to full information. Basic outcomes that are affected by appraisal and coping processes are functioning in work and social life, morale or life satisfaction and somatic health (Lazarus & Folkman, 1984).

In the primary appraisal process, an individual evaluates why and to what extent the person-environment relationship is stressful (i.e., harm/loss, threat and challenge). Note that a situation is not always evaluated as stressful; it can also be evaluated as irrelevant or benign-positive, respectively having no effect on or enhancing a person's psychological well-being (Lazarus & Folkman, 1984). When the situation is perceived stressful, an individual evaluates the options of how to deal with it in the secondary appraisal process. This is quite a complex process in which individuals not only need to consider coping responses, but also the efficacy of the coping response, one's self-efficacy related to performing the coping response and the possible costs of the response (Lazarus & Folkman, 1984; Maddux & Rogers, 1983).

As our study deals with victims – who are already confronted with a stressful situation – we are mainly interested in the coping process. Note that coping can take place before (threat anticipation), during and after events (Beaudry & Pinsonneault, 2005). Frieze et al. (1987) divide coping strategies into cognitive and behavioural coping strategies. Another division that is made when dealing with stressful appraisal is problem-focused coping and emotion-focused coping (Lazarus & Folkman, 1984).

Problem-focused coping aims to solve an undesirable situation by tackling the direct cause of a problem or threat. Lai, Li, and Hsieh (2012) identify two types of problem-focused coping in the information systems context: technological and

conventional coping. An example of the former is installing or updating anti-virus software to protect a device against future malware attacks. The latter deals with the behaviour that an individual displays without using technology, for example, checking the account balance for inconsistencies. Lazarus and Folkman (1984) define these as strategies directed at the environment and strategies directed at the self.

Emotion-focused coping aims to change undesirable feelings and emotions towards a problem or threat, such as stress, anger, fear, sadness and helplessness, without taking actions against the actual cause. Examples of emotion-focused coping include cognitive strategies such as avoidance, distancing and selective attention, and behavioural strategies such as meditating, seeking emotional support and having a drink (Lazarus & Folkman, 1984). Emotion-focused coping does not change the objective reality, but helps individuals to manage their emotions or control their emotional distress (Green et al., 2010), which is also important for effective coping (Lazarus & Folkman, 1984). However, such strategies can lead to a false perception of reality (Liang & Xue, 2009).

Emotion-focused coping is likely when an individual comes to the conclusion that nothing can be done about a situation, whereas problem-focused coping is more likely to be adopted when a situation is perceived to be changeable or controllable (Lazarus & Folkman, 1984). Liang and Xue (2009) state that rational individuals are likely to use problem-focused coping as a strategy because they probably have the required knowledge and the necessary skills to do so. If individuals, however, do not find a solution to mitigate a threat or if they adopt an ineffective measure (e.g., anti-virus software that cannot detect new variants of malware), then they will have to use an emotion-focused strategy in order to maintain adequate levels of psychological well-being. Furthermore, these strategies are not opposites per se; they may also complement each other. For example, installing anti-virus software is a problem-focused strategy to mitigate malware attacks, but an emotion-focused strategy is applied as well, i.e., hoping that one will not contract a malware infection (Liang & Xue, 2009). Moreover, problem-focused and emotion-focused coping influence each other, which can be either facilitating or impeding (Lazarus & Folkman, 1984). Thus, although the problem-focused strategy appears to be the preferred one – since taking actions against a threat or harm seems more meaningful than changing relational meanings (Liang & Xue, 2009) – emotion-focused strategies are also very relevant for effective coping.

The extent to which a victim is able to regulate emotions can result in the victim denying, nullifying or coping with victimization (Frieze et al., 1987). For coping

to be effective, it is important that individuals (in time) move beyond seeing themselves as a victim. The extent to which victims perceive themselves as victims depends on whether the situation is cognitively evaluated as a harmful stressor or not. According to Matthieu and Ivanoff (2006), a stressful event becomes a stressor when it is perceived to have a negative impact on one's personal well-being. Thus, regardless of what is objectively defined as victimization, 'victims' may not subjectively perceive themselves that way. Indeed, what some may consider stressful may not apply to others. This is primarily down to one's personal characteristics – some are more sensitive or vulnerable than others towards certain events – and the nature of the event (Lazarus & Folkman, 1984).

It is also important that victimization is recognized by others. This is, however, not always obvious, because the offence itself might be evaluated as a victimless crime (Button et al., 2014a). Additionally, victimization might not be recognized because of the perceptions people hold about what constitutes being a victim. The 'ideal victim', based on Nils Christie's definition, is likely to be female, sick, very young, very old, or disabled (or a combination of these attributes) (Dignan, 2005). When these attributes are not met, then the victim status will be less likely assigned, resulting in victims being given less recognition and/or being taken less seriously. In other words, the more innocent victims are perceived to be, the more likely it is for others to see them as victims. Similarly, if victims deviate from this image, i.e., when perceived to be not 'ideal', this will be less likely.

Additionally, the circumstances play an important part in making an ideal victim according to Christie's typology. When victimization is perceived unavoidable, people are more easily assigned the victim status. This is also the case when it is believed that victims engaged in practices they thought were legitimate and, therefore, can be considered blameless for what had happened. An unknown attacker, who is unambiguously evil, is also of significance. Finally, victim status is more easily assigned when victims display the right combination of power, influence and empathy (Dignan, 2005). The question is to what extent people believe online banking fraud victims to be truly innocent, as the victims – at least for phishing – adhered to what perpetrators demanded from them. The extent to which victims perceive themselves to be 'victim' and their perceptions on how others viewed them is, however, beyond the scope of the current study.

Coping efforts not only involve cognitive adjustments, but also taking action. Behavioural actions include locating the perpetrator (and demanding the stolen goods or compensation for what was lost, but also retaliation for what was done), target hardening (e.g., self-defence lessons, being more cautious,

installing alarm systems), avoiding social contacts (e.g., not leaving the home, moving to a new house, changing telephone number), seeking help from others (e.g., medical assistance, emotional support, assistance with physical tasks) and seeking help from the criminal justice system (Frieze et al., 1987).

Button et al. (2014a) report changes in victims' behaviour in a study of fraud. These include being more cautious when taking financial decisions, credit card usage and internet purchases, and being less trusting of others. It also leaded to positive changes towards the threat because victims became more security aware and attentive to fraud prevention. Regarding behavioural coping, two effective strategies found in a study on identity theft by Sharp et al. (2003) were taking actions to resolve the issue and talking to family and friends. The latter was found to be an effective means of coping for victims of other types of offline crime as well (DeValve, 2005; Frieze et al., 1987; Lamet & Wittebrood, 2009). Frieze et al. (1987) argue that social support is effective in protecting victims from different pathological states, making it a vital aspect of successful coping. The extent to which online banking fraud victims use this and other coping strategies – as well as the effects and impact they have experienced – are inventoried by means of interviews, which is presented next.

5.3 Method

Semi-structured interviews were chosen as the research method to study the effects and impact of and coping responses to online banking fraud victimization. A topic list was developed based on a literature review. Although we tackled all of the topics in the interviews, in each interview the structure was modified to best fit the experience of the participant. The interviews were conducted face-to-face on a location decided by the interview participant. This was either at their home or at their working location.

Our aim was to identify the effects and impact of online banking fraud incidents and the coping responses after the incident. The questions were newly developed for this study and included: What is your experience with online banking? What effects did the incident have on you? Did the incident result in emotional harm? Do you recall the amount that was stolen? Did your bank reimburse the financial damage? Have you taken new or additional precautionary measures since the incident? Furthermore, demographic characteristics of the participants were registered. During the interviews, participants were also asked about how the incident had unfolded, possible reasons for being targeted and what protective measures they had in place. Outcomes of these particular questions are described in the work of Jansen and Leukfeldt (2016). The interviews lasted 52 minutes on average and were recorded using a digital voice recorder.

The participants were selected based on police reports and were contacted by a liaison officer working for the Dutch police to inform them about the study and to obtain their consent for voluntary participation in an anonymized interview. Of the 65 police reports selected from the northern and southern regions of the Netherlands, 29 participants agreed to be interviewed, 9 declined the request and 11 were not reached. Possible participants in the remaining 16 cases were not contacted because we obtained sufficient data to complete our study. One participant was recruited via a liaison officer at the Fraud Helpdesk, bringing the total number of participants to 30. The Fraud Helpdesk is a national organization for answering questions and collecting reports about fraud. The participants were interviewed between October 2014 and April 2015. The participants that were recruited based on police files were victimized in the year prior to the interview. The participant that was recruited via the Fraud Helpdesk was victimized three years prior to the interview. In this study, participants were defined as victims when they actively or passively gave away their user credentials because of phishing or malware attacks. In addition, the reports were not made available to the researchers by these organizations, making it impossible to triangulate the data.

The ages of participants ranged from 23 to 89 years (M = 59, *SD* = 17). Thirteen women and seventeen men were interviewed for this study. The distribution of their educational level – based on the grouping of Statistics Netherlands – was low (N = 3), medium (N = 15) and high (N = 12). The majority of participants were experienced users of online banking having used it for five years or more (N = 23) and using it at least once a week (N = 21). Their bank accounts were held at different banks in the Netherlands. In total, seventeen phishing victims and thirteen malware victims were interviewed – the cybercrimes of interest in this study.

The victim sample included private as well as corporate customers. For phishing, the distribution was sixteen to one. For malware, the distribution was one to twelve. The corporate customers were primarily self-employed entrepreneurs and small and medium-sized enterprises. Two of the malware participants were not the actual victims. Instead, we spoke with the partner of a victim and a supervisor of an employee who was victimized. We decided to include their input in the analysis because their stories contained relevant information, for instance on the financial impact and on changes due to the incident.

After the interviews were conducted, the recordings were transcribed and sorted into conceptual themes that we defined prior to the study. These were based on the research and interview questions, derived from general theoretical concepts, and include, for example, effects and impact. The interview data were analysed

using QualiCoder (Version 0.5), a type of computer-assisted qualitative data analysis software. Using this tool, we labelled the written information with analytical codes, which gave us the opportunity to separate the themes into more detailed categories (Ritchie, Lewis, McNaughton-Nicholls & Ormston, 2014), for example, psychological and emotional effects. Thereafter, the contents within these categories was gradually specified into codes, including, for example, feeling awful, stupid and disbelief. Finally, the output was manually recorded in a Microsoft Excel file, which can be shared upon request. A short summary of the interviews is provided in Appendix II.

5.4 Results

In the following sections, we present damage amounts (rounded up to hundreds of euros) and incidence of particular views or experiences of participants. We do not claim that we are providing a representative reflection of online banking fraud incidents. That is not possible using this interview method nor was it the objective of our study. Rather, it aims to provide insight into how coping phenomena vary among participants. Where possible, we make a distinction between the phishing and malware cases. Differences between phishing and malware are mentioned only when certain outcomes were reported for either one of the two fraudulent schemes. If only one participant mentioned a certain outcome, the response is not quantified, i.e., no N is indicated. Before we continue with the results, we provide a summary of a phishing and a malware case, because these give a good impression of what the interview participants have experienced.

Phishing attack – A participant received a deceptive e-mail containing a message to execute a security update for online banking. She clicked on the hyperlink that was included in the e-mail which re-directed her to a false website where she entered some personal details. About two weeks later, she received a fraudulent phone call. During the telephone conversation, she followed the instructions of the caller and passed on user credentials by which the fraudster used to log in and make illegitimate bank transfers.

Malware attack – A participant noticed at some point that the online banking screen "shook" briefly when being used (interview 30). At a later date, the participant wanted to transfer money to the Dutch Tax and Customs Administration. However, in the background, the transfer was split into two transfers (adding up to the same amount), of which the largest amount was sent to an unknown account and a smaller amount to the administration service. During the execution of that particular money transfer, the participant noticed nothing out of the ordinary. The split-up money transfer was not visible in the payment summary screen when using the compromised device. Based on an

investigation carried out by the Dutch police, we know that the malware was automatically installed on that particular device when visiting an infected website (Leukfeldt, Kleemans, & Stol, 2017).

5.4.1 Financial impact

Fifteen out of seventeen phishing victims reported that the incident caused financial damage. The total damage that these fifteen reported was 181,300 euros (M = 12,100; Min. = 900; Max. = 50,000). Seven of them were fully reimbursed by their bank. Three were fully reimbursed less a mandatory own risk excess of 150 euros, which one of the participants called a "fine" (interview 18). One participant received 1,000 euros from her bank, which was less than a third of the total damage of 3,600 euros. Four participants received no financial compensation, leaving a total damage of 58,700 euros. Two of the seventeen participants reported no financial damage, as their banks were able to immediately stop the fraudulent transfer. The amounts that the fraudsters were attempting to steal were 2,000 and "over 10,000" euros.

We asked the participants who were not or not fully reimbursed about their opinion of this. The participant (interview 6) who got back 1,000 of 3,600 euros mentioned that, according to her emotional response, this amount was not proportionate. However, she thought that it may have been the maximum amount that could be refunded. In addition, she found the whole experience "a terrifying adventure" and so she made no further attempts to reclaim more money. "I was restless, frightened, tense. Maybe I should have stood up for myself?" Rationally, however, the participant stated that she does understand why she was not fully compensated. "Not intentionally, but unintentionally, I was as stupid or as trusting as one could be." Because of the incident she had to cut her spending, for instance, by not going on holiday.

The participants who were not compensated at all expressed different views. Three of them respected the fact that they did not receive any compensation, stating that it was their own fault. One of them mentioned, "I did it to myself. So be it. I cannot turn things back. It is just silly, silly, silly" (interview 12). The second participant said, "It is the same as when you drive though a red traffic light. Then you get fined; it is your own fault. And that is also true in this case" (interview 13). She tried to minimize the impact by stating that, "It could have been more [money]." The third participant stated that he understood that he made the error, although he thought that the bank could have done more to trace the suspects.

The fourth participant (interview 15) who received no compensation was "very sorry" that she was not compensated, especially since "banks are so big." She

felt that, because of the compulsory nature of online banking – "in particular for elderly people" – the bank could have shown more goodwill, also given the many years that she had been a customer of that particular bank. Her rationale was, however, that the bank could not compensate her "because there are perhaps too many [phishing] cases." She also mentioned to have lost her security, i.e., having a monetary buffer, which affected her significantly. When talking about it with her husband, the impact was minimized for her because he made clear to her that they are still able to eat.

Twelve of the thirteen malware victims reported that the incident caused financial damage. One participant did not mention the amount that was stolen. The other eleven participants reported a total damage of 52,800 euros (M = 4,800; Min. = 1,000; Max. = 10,000). All twelve participants were fully reimbursed by their bank. One participant claimed, however, to have lost out on interest during the time that his money was not in his bank account. In one of the thirteen cases, there was no financial damage because the bank was able to block the fraudulent transfer immediately. The participant mentioned that the amount that the fraudsters were attempting to steal was about a monthly wage.

5.4.2 Psychological and emotional impact

Most participants reported that the event had at least some psychological and/or emotional impact on them. Four participants, however, expressed no psychological or emotional impact. The supervisor of a malware victim stated, "It is all in the game. It is part of life, running those risks. […] And, besides, it is only money. If physical violence was involved, then it would have real impact" (interview 28). Three of these four participants indicated that they would probably have assessed the impact differently if they had not been compensated by their bank.

Eleven participants reported that the incident did have an impact, but that it was low. A malware victim mentioned that, "It is an administrative thing" (interview 21). Although he still felt "screwed," he did not worry about it, because he knew that the money would be back within a week. Another malware victim said, "You have a strange feeling, but nothing more. The intangible makes it difficult. With burglary, you see that things are broken and ransacked" (interview 23). Three phishing victims said that, although they did not experience any psychological or emotional impact or only to a small degree, they were annoyed by it.

Some participants compared online banking fraud with burglary (N = 2), while others believed that a comparison with burglary is not possible (N = 5). On the one hand, a phishing victim stated, "Strange people just enter your private life, and that is the most disgusting part of it. It does not matter if it is on your

computer with money, or that people steal your belongings or are only sniffing around and turn things upside down. It just gets to you" (interview 2). On the other hand, the spouse of a malware victim mentioned, "Hacking into your computer is a totally different experience. Burglary at home is a violation of your privacy. In this case, it is a technical thing" (interview 25).

Participants who experienced psychological and/or emotional effects said that, in general, they felt awful (N = 8), disbelief (N = 8), fear or shocked (N = 6), stressed or nervous (N = 6), cheated (N = 4) and insecure (N = 3). It also lowered their trust in banks and/or online banking (N = 8). An effect mentioned only by malware victims is being misunderstood (N = 2). Effects that only phishing victims mentioned included feeling stupid (N = 8), shame or embarrassment (N = 5), angry (N = 2), devastated (N = 2), sadness and feelings that things are deprived. Phishing victims also stated that the incident lowered their levels of trust in themselves (N = 3) and in people in general (N = 2). A participant pointed out that, "If you lose your trust, you lose more than your trust, you lose your certainties. […] I trust all people to be honest and open. That trust has been given a big blow. When I say that I could cry again, since I find it that terrible. I still suffer from it" (interview 12).

Furthermore, phishing victims mentioned that the incident made them feel less safe online (N = 4) and offline. The participant who mentioned feeling unsafe both online and offline said that these feelings were linked to a previous life event in which she was cheated. "Those feelings came back through this phishing incident. It really knocked me off balance. It certainly took a month. I was just really scared" (interview 6). She reported that the incident also affected her sense of safety in her home. She asked herself whether the criminals who had scammed her might have obtained her physical address. She indicated having had sleepless nights, wondering whether people would sneak into her home. "You don't know how far it may reach."

Other phishing victims also mentioned having suffered from physical effects. One participant (interview 17) spoke about having "a trauma" and mentioned also having suffered from sleepless nights. "This was less about the money aspect, but more about the stupidity." The participant blamed himself that he fell for the scam. "You lose your self-confidence, because you can be so stupid." Contrary to this statement, four participants stated that the incident was something that befell them. A malware victim indicated that, "You must make sure that you don't blame yourself. You don't have control over it" (interview 30).

One of the phishing victims indicated that, "Its aftereffects are very bad. It has had a lot of impact and still makes me feel very sick" (interview 12). One aftereffect that she mentioned was that she experiences black outs from time to time. Another phishing victim claimed that she almost collapsed when the incident happened. She mentioned having had heart palpitations when the bank e-mailed her with the message that she would not be compensated for her financial losses. She felt terrible and could not believe it. During the process of getting her money back, she became very insecure. "When I was using online banking for the first time after the incident, I was shaking all over" (interview 1). She reported being very anxious, mostly because she no longer felt in control. Furthermore, it influenced the work she is doing for a foundation. She is the treasurer of that particular foundation, but because of the incident she finds it terrifying and wants to resign from that role. "The idea that this [a successful phishing attack] would happen to me with other people's money makes me feel sick." Finally, a malware victim indicated that he was shivery using online banking after the incident, but that this feeling was subsiding as time passed.

The duration or timeframe of the effects was also mentioned in some of the other interviews. In total, four phishing victims stated that the effects are still (partly) present. Participants indicated for example that, although the incident had happened a while ago, feelings of uncertainty or distrust, especially with regard to digital payments, still exist to this day. One participant mentioned that she is trying to get over it, which she is confident about, as "time heals all wounds" (interview 6).

Seven participants reported that the impact goes away or at least goes into the background. A phishing victim reported that the impact lasted for two or three days. When things were back in order, she turned the page. Another phishing victim reported that feelings of shame and stupidity have subsided over time, but that it is not one of his favourite topics of conversation. "I don't talk about this topic at parties. It was quite an impactful experience" (interview 3). Two others also mentioned not sharing the experience.

Some, however, did (occasionally) talk about the incident within their social sphere (N = 13). Most did this for coping purposes, but five of them also did so to warn people about such schemes. In two out of thirteen cases, participants mentioned that the people they told about their experience tried to help them to get their money back and to locate the people responsible for the scam. Another participant indicated that the positive aspect was that her fellow residents from the elderly home and her family supported her really well, which helped her to cope with the incident.

5.4.3 Secondary impact

Some of the participants reported that the negative event also had secondary impact. This was often related to the handling of the incident. Obvious ones were time loss due to reporting the incident to both the bank and the police, a blocked bank account and, consequently, not being able to having direct access to their own money. A malware victim indicated that the time between the incident and reimbursement of the bank was bothersome. "As a self-employed entrepreneur, you don't feel like spending hours on phone calls with your bank during the day" (interview 9). One phishing victim mentioned, "Especially as you get older, you don't want to be bothered by such things" (interview 4). Although this section mainly deals with negative experiences, nine participants explicitly mentioned adequate levels of expertise at the bank and/or the police and mentioned that they took it seriously and were understanding and helpful. One of them mentioned that this attitude was very reassuring.

Other types of secondary impacts that were mentioned by participants from both fraudulent schemes included feeling mistreated (N = 6), bad communication (N = 4) and an uncooperative attitude (N = 3) on the part of banks. A phishing victim felt mistreated by her bank when reporting the incident. She got the impression that the bank employee sitting across her was thinking, "'Oh, you are so stupid.' He made that very clear" (interview 1). Participants also felt that they were being treated like the guilty one, or felt as though they needed to prove their innocence.

All of the participants went to the police to file a report. In nineteen cases, participants were obliged or advised to do so by their bank. Eight reported having done so on their own initiative. Of the remaining three cases, we do not know what motivated them. Secondary impact related to the police were reported as follows: the police initially not wanting to or not having time to file the report (N = 5), having to wait for a few days (N = 3, in one case because the right person was unavailable), having to drive far to a police station and a lack of expertise that was displayed by the particular police officer. The participant of the latter case – a malware victim – stated, "The person who filed the report did not understand any of it. You cannot blame that person for not knowing everything, but the police can significantly improve in this regard" (interview 21).

Two phishing victims mentioned that they received many payment reminders during the time their bank account was blocked, which they found annoying. Two malware victims mentioned having to settle things because of the fraudulent transfer. One of them needed to settle things with the Dutch Tax and Customs Administration, because the participant's business received a formal

warning. She had to rectify things by reporting that the late payment was unintentional, that was due to a fraudulent attack. The other participant needed to settle things similarly with a DIY store.

Finally, five participants indicated that either the police or their bank updated them about the incident. In two instances, it concerned a standard message that there were not enough leads to continue working on the case. In one instance, a malware victim mentioned being updated on the case by a police detective. This had a positive effect on the level of trust that something was actually being done. Some of the participants that mentioned not being updated made them feel they were being left in the dark or gave them the impression that nothing was done about their case.

5.4.4 Behavioural change

We asked participants whether they had changed their behaviour due to the incident in order to cope with the incident or to prevent future incidents. We have categorized behavioural change into three categories: (1) behavioural change related to devices used for online banking; (2) behavioural change related to online banking sessions; and (3) behavioural change beyond the online banking context. It is important to note that we have relied on self-reported behavioural change. We have no additional data that provides support for what the participants told us.

Behavioural change and devices

Seven participants told us that they had installed an additional anti-virus or anti-malware package, such as Malwarebytes and TDSSKiller. Four participants reported having changed their anti-virus software, of which one indicated that the device had no anti-virus software during the time of the incident. Another participant switched from a free package to a paid package, in order to prove to the bank that he is doing a good job. Three participants said that they updated their software more frequently. A phishing victim reported that her computer now updates every night and that she manually checks for updates once a week. This was not only due to the incident, she received messages from her bank stating that financial losses caused by phishing will not be reimbursed if software is out of date.

Other changes that were mentioned more than once were no longer using the device that was used during the incident (N = 2) and buying a new computer (N = 2). The latter was only reported by malware victims. One of them mentioned that the police advised her to buy a new computer. This additionally led to the IT staff needing to reinstall all the (business) software. She mentioned, “We have no insurance for that” (interview 30). Changes that were mentioned once

included using a different web browser, switching from a Windows desktop to an Apple iPad (which was perceived to be safer) and replacing the hard drive of the compromised device with a new one.

Behavioural change and online banking

More than half of the participants indicated that they had become (extra) alert or more aware of phishing and malware attacks (N = 17). Participants also indicated that the incident was a good learning experience (N = 14). In addition, participants had changed their online banking practices. Being more careful/meticulous or taking more time to properly check what they are doing during online banking and online purchases (N = 8), checking the account balance more regularly (N = 7) and checking the security certificate (N = 7, e.g., https, closed padlock) were mentioned by both phishing and malware victims.

Changes that were reported only by phishing victims include logging out of banking sessions instead of clicking away the window (N = 3), checking the web address (N = 2), using online banking less and traditional banking methods more when transferring money (N = 2) and not using online banking at home anymore. In this particular case, the participant visits a local bank once a month to conduct his banking activities. If he is not sure about something, he can ask a bank employee to help him.

A new online banking practice that only malware victims mentioned was taking screen shots of their online banking activities (N = 2). One of them mentioned doing this, "To be able to prove that you are doing the right thing" (interview 23). After about a year, both participants stopped doing this. Another participant mentioned that when she had to transfer large amounts of money, she would contact the bank by phone to find out if everything was in order. She attributed this to her insecurity that was caused by the incident. However, she soon stopped with this procedure, because it was not practical.

Besides the duration of the new behaviours mentioned above, the timeframe of the new behaviour was also mentioned in a few other cases. Three malware victims mentioned that being extra alert or more careful was already waning. Two phishing victims who stated that they check to see if there is a closed padlock revealed that they do this less frequently now or not at all anymore. Finally, a phishing victim disclosed that she no longer checks the account balance regularly.

Behavioural change beyond online banking context

One frequently mentioned change in the behaviour of phishing victims beyond the online banking context was that they became more suspicious about e-mails (N = 8), for example, not clicking on hyperlinks and checking whether e-mails are trustworthy. One also commented that it has become difficult to differentiate between legitimate and false e-mail messages. Other phishing victims mentioned to deleting all e-mails that are or seem to be sent by banks (N = 4). Two also commented that if the message is important, the bank would have sent a letter.

Six phishing victims made changes to their bank accounts. Changes included removing the credit limit from the account (for overdraft protection), configuring the debit card so that it cannot be used abroad, receiving a different bank account number from the bank (because fraudsters carried out new phishing attempts), closing a savings account (because that particular account was protected by a password only, which seemed to be unsecure), opening a savings account at another bank (since the checking and savings accounts had the same numbers, which was perceived to be unsafe) and opening several bank accounts (where specific amounts of money can be deposited, leaving only a smaller amount in the checking account). In this particular case, the participant commented, "In this way, third parties cannot get to the big money" (interview 16).

Four phishing victims said that they are more on guard when using mobile phones and receiving telephone calls. Three of them mentioned that if the phone's display does not show a number, they pick up the phone without stating their name or they do not answer it at all. The other participant got himself a new phone number. Furthermore, two participants intended to leave their bank, but did not follow through.

Changes that were mentioned just once by phishing victims included not buying or signing anything anymore at the door, not writing down the PIN code in an agenda or on a piece of paper, not giving out their bank account number as readily as before and not going on the computer when feeling sad (for this participant, safety is embedded in sadness). A participant who was phished while being the treasurer of a foundation indicated that the foundation had invested in making its website more secure.

Two malware victims commented that they had made changes beyond the online banking context. One of them mentioned that business procedures and protocols were carefully re-examined in order to make sure that incidents would be adequately prevented or detected as soon as possible. Another indicated not

sending information from business computers to the main business computer (used for online banking), i.e., not running any unnecessary risks.

5.5 Conclusion and discussion

Although we believe that our study provides a unique contribution to literature, our study has its limitations. First, the results are not generalizable for all online fraud victims. We focused on victims who suffered from online banking fraud only. Furthermore, the participants were selected from police files. Therefore, we do not know what the effects are on victims who did not report the crime or how they cope with such events. Reasons for non-reporting include, for example, not knowing to be defrauded, feeling partly responsible, feeling embarrassed and suffering low financial losses (Button, Lewis, & Tapley, 2009b). This limits generalizability, also because reporting rates are low.

In 2015, for example, 2% of all hacking cases, 20% of marketplace fraud cases and 13% of identity fraud cases that Dutch people were confronted with were officially reported to the police (CBS, 2016b). Perhaps in-depth interviews that follow a crime survey could be a way to address this limitation. Moreover, some potential participants declined the request to be interviewed. Perhaps these victims did not participate because they perceived higher or more problematic psychological and emotional impact than those in the sample. Another possibility is that these victims were not affected at all, and therefore had no interest in participating. What becomes clear though is that victims vary in their characteristics and profiles. This concurs with previous research on fraud victimization (Button, Lewis, & Tapley, 2009a; Button et al., 2009b; Cross et al., 2016).

A possible limitation is related to the identification of psychological and emotional effects. Although we found that the participants talked openly about these and other subjects, the participants may have hidden some of these effects from the researchers because they felt too embarrassed about it. Dignan (2005) stresses that it is very difficult to measure such effects because the willingness and ability of people to talk about these issues, as well as about the experience itself, are highly subjective and partly cultural specific. This also counts for coping efforts because people are not always aware of what they are doing exactly (Lazarus & Folkman, 1984). The subjective nature of this study may therefore have led to the problem of method variance. Lazarus and Folkman (1984), however, nuance the problems of validation by stating that subjective reports allow researchers to learn more about coping than any other single source. In order to make outcomes more comparable, regardless of their subjective nature, we recommend using other specific assessment tools in future

studies, for instance, the 'ways of coping' checklist (see Lazarus and Folkman [1984]). However, this would require a more quantitative research approach.

Finally, the current study adopts a retrospective approach, which has its limitations (Shapland & Hall, 2007). Participants may have forgotten certain details about the effects of online banking fraud and how they cope or coped with these. We have gained an impression of the short-term consequences, but we do not explicitly understand how victims' coping strategies pay out in the long term. Some participants, for example, mentioned that they were already using some behavioural coping measures less frequently. It would be interesting to find out whether individuals are consistent or variable in their coping strategies, and what their overall coping style is, as opposed to our more contextual focus on coping efforts (Lazarus & Folkman, 1984). Indeed, coping is not a one-off activity. Future studies could benefit from a longitudinal approach. Studying the effects and impact that victims perceive, and their cognitive and behavioural responses at multiple points in time provide richer data with more potential, for example, to understand how perceived effects develop and to better guide a victim through the coping process. Further research may also benefit from investigating personal, psychological and contextual factors that affect coping efforts.

The first research question we wanted to answer is: What are the financial, psychological and emotional effects of online banking fraud victimization? We start with the financial effects. Most participants experienced some financial damage – at least initially – from either phishing or malware victimization. Two thirds of the phishing victims and all malware victims whose bank accounts were affected were fully compensated for their financial losses. That all malware victims were fully compensated has probably more to do with the type of the offence, that is the obscureness of the malware attack, than with the observation that most were corporate customers. Imaginably, the circumstances surrounding malware victimization appeal to the 'ideal victim' typology.

Five participants – all phishing victims – were not or to a minor extent compensated for their losses. Although the participants who suffered financial losses acknowledged that being victimized was to some extent due to their own wrongdoing, some expected more goodwill from their bank regarding compensation. Moreover, it would be interesting to investigate the banks' reimbursement policies on this matter: why are some phishing victims compensated, be it in full or not, while others are not?

Besides the direct financial effects, indirect financial effects were also reported. These effects included loss of interest, buying a new device for online banking

and several types of loss of time that can be considered to have a monetary value, such as devoting more time to taking precautions (online) and going to a physical bank office to use banking services. Thus, the financial effects go further than only the (initial) damages caused by the fraudulent schemes.

We will now turn to the psychological and emotional effects. The participants that mentioned that the event affected them psychologically and emotionally mentioned a range of effects, such as feeling awful, stupid, stressed, disbelief and fear. It also affected their levels of trust, including trust in banks and/or online banking, people and themselves. That such psychological and emotional effects follow victimization is consistent with other research on (online) fraud (Button et al., 2009a; Cross et al., 2016). Some participants even reported physical effects, such as having sleepless nights, getting heart palpitations, experiencing blackouts and feeling shivery or shaky when using online banking.

We also found some evidence regarding the duration of the effects (Frieze et al., 1987). Most participants mentioned that they had immediate reactions to the incident. The psychological and emotional effects were often at their most severe during this particular timeframe. Some of the participants mentioned that the effects subsided after a few days. Some, however, reported that the effects or impact experienced lasted from about a month to still being present at the time of the interview. This is a similar pattern that is observed for (offline) violent crimes (Dignan, 2005) as well as for different types of online fraud (Cross et al., 2016).

The second research question was: To what extent do online banking fraud victims suffer from secondary victimization? Secondary victimization relates to negative effects other than those instigated by the incident itself. Negative effects often related to the way the incident was handled, such as time loss due to reporting the incident, not being able to access the bank account and feeling mistreated. Feeling mistreated has a negative influence on coping because it does not address the victims' need for recognition.

In addition, most participants mentioned that they did not receive feedback from either the bank or the police on the incident and how it was being handled. Frieze et al. (1987) argue that such information helps victims to relieve their fear and frustration, thus helping them in the coping process. In addition, victims may develop a positive attitude towards banks and the police instead of losing their trust and confidence in these organizations. The study of Button et al. (2009b) also found that fraud victims have a need for being held up-to-date on the process of the case. We believe that providing feedback, not only on the

status but also on how the incident happened, can help victims to develop more effective defence strategies against future attacks.

Besides negative effects, some participants explicitly reported positive aspects in the handling procedure. They mentioned that bank employees and police officers took them seriously, were understanding and helpful, and had adequate levels of expertise for the situation. Again, banks and the police stand to gain a lot if they respond in this way, not only reputation-wise, but also when it comes to helping victims to recover properly from online banking fraud victimization.

The third research question was: What impact does online banking fraud have on its victims? Although the financial 'effects' of online banking fraud could objectively be defined as quite severe, the participants did not claim that the incident had a devastating financial 'impact', which is sometimes the case for other fraud victims (Button et al., 2014a). Therefore, we conclude that the direct financial impact of online banking fraud victims is low, most notably because the majority of victims were compensated for their losses. This differs from other types of fraud, where it is often more difficult or even unlikely to get restituted (Button et al., 2009b). Remarkably, some of the participants who were not compensated at all also felt that the impact was low. Three participants had no financial damage to begin with.

Regarding the psychological and emotional aspects, four participants said they felt no such impact. This was also mainly due to the fact that they were financially compensated for their losses, but also because online banking fraud was considered a technical or invisible phenomenon. These participants felt that their private lives had not been affected. About a third of the participants mentioned that the 'impact' of the fraudulent attack was low, but did express some psychological and emotional 'effects'.

Half of the respondents were – to some extent – overwhelmed by the situation. Thus, reimbursement could not prevent some of the participants from being psychologically or emotionally affected by the incident. Furthermore, we found some evidence that previous negative life events affected the impact of victimization. Our topic list, however, did not include questions about such events or prior victimization, which could be beneficial to add in future studies. Similarly, questions could be asked whether or not other accounts beyond banking were hacked, which may also have affected the impact experienced by participants.

The final research question was formulated as follows: What are the cognitive and behavioural coping responses to online banking fraud victimization?

Regarding the participants who were not compensated, or not fully compensated, for their financial losses, we observed that they used a cognitive coping style of rationalizing it, thereby minimizing their victimization. They came up with an explanation that seemed to fit the situation in order to cope with the fact that they had lost their money.

Cognitive coping strategies were also observed regarding the psychological and emotional effects of becoming an online banking fraud victim. Examples included being at ease with the situation because reimbursement procedures were understood, and viewing an incident as being something that is part of life. Some participants tried to create a 'hypothetical, worse world' scenario in order to cope with victimization (Taylor, Wood, & Lichtman, 1983), for example, by thinking that the stolen amount could have been higher or that it would have been worse if it had involved physical violence. These strategies are effective for reducing emotional distress, but ineffective for tackling the actual problem.

Another cognitive coping response is that victims feel strengthened by the experience. Some indicated that the experience was a good lesson in that it made them wiser, which is also considered to be positive change in other studies (Button et al., 2014a; Whitty & Buchanan, 2016). Perhaps confronting online banking users with (controlled) phishing and malware attacks would be a good strategy as a way to teach them how to prevent such attacks.

A strategy that makes coping difficult was observed in a participant who blamed himself for being victimized (Whitty & Buchanan, 2016). Although self-blame can be considered a maladaptive response, which could for instance lead to hopelessness and depression, it can also be considered an adaptive response if self-blame is considered to be behavioural. If victims are able to link their own actions to victimization, they can avoid future victimization by adjusting these actions. On the other hand, if victimization is linked to character, it gives victims less confidence in their perceptions of avoiding future victimization because personality is hard to change (Frieze et al., 1987).

Some participants reported an opposite strategy towards self-blame, indicating that the incident was something that befell them, which helped them control their emotional state. In our opinion, this is not a strange – and perhaps the right – reaction, as the skills of fraudsters are often the reason why people fall for such scams. Individuals that are victimized are not stupid; they simply made a choice that was not a good one. For malware victims, it was out of their hands,

because their systems were infected automatically.[38] For these victims, the cases remained unsolved; they do not know how their systems were infected nor how the fraudulent transfer(s) took place. They were surfing online in the wrong place, at the wrong time. In general, this did not cause any distress, most probably because all were reimbursed – which might have strengthened their belief that they could not help it.

Respondents also applied behavioural coping mechanisms. The first behavioural coping mechanisms that they applied was reporting the incident to and seeking support from their bank. In addition, all participants filed a report with the police (which is logical given our selection procedure), either because the bank required them to or on their own initiative.

Some participants also sought support from their social environment, which was assessed as an effective means of coping. This is also identified in the literature as one of the most effective means for successful coping (Frieze et al., 1987). One of the participants mentioned after the interview that the conversation had a healing effect on her, as she had not talked about it much. According to her, banks should provide aftercare in the form of having a conversation about the event after some time, helping victims to process it. Were banks to follow up on these incidents, it is essential that the person instigating the conversation adopts a supportive attitude, i.e., be unprejudiced, show empathy and understanding – not blame the victim, as the situation itself is difficult enough.

However, it can remain a difficult topic to address for some time. Perhaps these participants are assuming that others might find them stupid or that they would be angry with them because of the financial loss. Indeed, according to Cross

[38] This study includes both phishing and malware attacks, because they are basically two types of the same crime. Leukfeldt, Kleemans, and Stol (2017), for example, show that not only the goal of phishing and malware attacks is the same (i.e., to steal money from online bank accounts), but that the modus operandi of both attack types is quite similar too (intercepting login credentials, intercepting one time transaction authentication codes, wiring the money to money mule accounts and cashing the money). The biggest difference is that the malware victims in this study were not actively engaged in providing perpetrators their credentials. However, being fully responsible or not, it is still relevant to find out how the malware attacks affected participants and how they recovered from it. Furthermore, we had no information on how well the victims were protected against malware attacks before conducting the interviews. Personal responsibility could have been an issue when we had found that malware victims, for instance, had poor security protection installed. Moreover, in other malware cases, victims were more personally responsible, for example, by responding to a malicious pop-up window (see e.g., Jansen and Leukfeldt [2015]).

(2015), there is a negative vibe surrounding online fraud victimization, although she found that phishing is a more acceptable type of fraud victimization, than, for instance, advance fee fraud and romance fraud. Whitty and Buchanan (2016) argue that negative or non-supportive responses from the social environment can be harmful for recovery. We found no evidence that online banking fraud victimization affected social relationships, nor did we find any leads indicating indirect victimization by people within the victims' social environment. Perhaps this is the case, because the research participants were open to share these experiences with the people closest to them. Other fraud research has shown that when such events, for example, are kept secret the impact on partners and family members can be more severe (Button et al., 2014a).

We also identified environmental strategies and strategies directed at the victims themselves. Environmental strategies included installing a different or additional anti-virus package and (more regularly) checking for software updates. A frequently mentioned strategy that was directed at the victims themselves was that participants became more alert to or aware of phishing and malware. Being more cautious after victimization is also found in the fraud studies of Button et al. (2009a; 2014a) and Cross et al. (2016). Online banking processes were also adjusted, such as being more meticulous or taking more time to check things, checking the security certificate and checking the account balance more regularly. Furthermore, we observed that some participants adopted avoidance behaviour, i.e., using (or wanting to use) online banking less and using traditional banking services more.

Some of the abovementioned strategies can be considered to be problem-focused coping, as they are intended to prevent an online banking fraud incident from happening again. However, these strategies could also be adopted as a means to control emotions, for example, making them feel more confident about online banking. It is therefore difficult to determine whether certain responses belong to problem-focused and/or emotion-focused coping strategies (Lazarus & Folkman, 1984), so we have not labelled them as such. Follow-up research is required to clarify in greater detail how these strategies work.

Finally, we found that participants also performed behavioural coping strategies beyond the online banking context. One frequently mentioned example is that phishing victims reported being more concerned about or suspicious of e-mails. As a consequence, it was mentioned that it is often difficult to differentiate between legitimate and false e-mail messages. This is also observed by Wang, Chen, Herath, and Rao (2009), who note that phishing has a high impact on legitimate commercial e-mails. Other responses that phishing victims mentioned

more than once included making changes or restrictions regarding bank accounts and being more on guard when taking telephone calls.

Concluding remarks

We agree with Button et al. (2014a) that, similar to other types of fraud, online banking fraud cannot be considered a *victimless* crime, not even when the stolen money is reimbursed (see also Whitty and Buchanan [2016]). The effects and impact of such fraudulent schemes on victims should not be underestimated. Regardless of the financial costs associated with online banking fraud, losing trust (e.g., in online commerce and people in general) and declining levels of safety and security are a much higher price to pay. However, the extent to which an individual perceives these effects and impact differs significantly. For some it was a temporary inconvenience only and they managed to get over it, whereas for the other it was (and sometimes still is) an overwhelming experience that changed them; they became more attentive, alert and distrustful as a result. This means that individual differences should be acknowledged when helping victims to cope with their victimization. Hence, for help to be effective, one should take into account the interplay between personal characteristics and the environment (Lazarus & Folkman, 1984). They went on to state that effective help can only be achieved if a process-oriented view is adopted. This would involve examining what happened and what is happening to that particular individual in terms of coping.

This conclusion has implications for banks and law enforcement agencies. Banks primarily have to deal with the incident and the damage resulting from the incident. Banks could probably improve their services by recruiting dedicated personnel who devote attention to the victims' coping process, employees who are able to assess how the victims' coping process is unfolding and who can support these victims in that process. These employees could have contact with the victim at multiple points in time, depending on the specific needs of the victim. This may require a different set of skills than those that bank employees at fraud departments currently have.

Another strategy might be to cooperate with 'victim support', a service that is provided to victims when they report a crime to the Dutch police. An important implication, also for law enforcement agencies, is that victims should be treated seriously and that the impact they experience goes further than the money aspect only. It is crucial to do this right on the first time victims come into contact with these agencies – when reporting the incident – because this might set the tone for the whole handling procedure. Moreover, as pointed out by Cross et al. (2016), a negative reporting experience can worsen the harm that victims already undergo. To evaluate whether this is done adequately and to

continually improve the support of victims, it is recommendable to map the customer experience in terms of fraud handling, which is already done by different banks in the Netherlands (personal communication, April 26, 2017).

Conclusively, we have contributed to the literature by increasing insight into the effects and impact of phishing and malware attacks and enhancing the understanding of adaption after online banking fraud victimization. These aspects are currently lacking in studies on cybercrime. More thorough analysis of coping strategies is required to deepen insight into the phenomena described in our study. This is not only needed to advance theoretical knowledge on this topic, but also to further shape the supporting role that banks and law enforcement agencies have, as presented in the recommendations above. We need more information about the factors that cause stress, how coping strategies are chosen, which strategies are effective and which are not, and how these function over time. Some coping efforts seem to work for a while, but subside over time as they seem to hinder usability, cost too much time and some perhaps do not work at all.

PART II:
PRECAUTIONARY ONLINE BEHAVIOUR

CHAPTER 6

Comparing three models to explain precautionary online behavioural intentions

Jurjen Jansen

Paul van Schaik

Published in Information & Computer Security 2017, 25(2), 165–180.

6.1 Introduction

Today, society is becoming increasingly networked and connected (Van Dijk, 2012). As more services to customers are offered online, such as banking, government and health, security becomes increasingly important. Individuals, economy and society can be harmed when security is compromised, for example, by means of data breaches and distributed denial-of-service attacks. The Netherlands' first National Cybersecurity Strategy states: (secure) IT is fundamental for our prosperity and well-being and essential for economic growth. This means that besides increasing the adoption and use of IT, it is equally important to ensure its safety and security (Dutch Ministry of Security and Justice, 2011). It is evident that societal issues, like cybersecurity, need to be addressed by different parties, such as internet service providers, telecom organisations and governmental agencies. However, it is equally important that end users behave in a secure fashion, as they play an essential role in safeguarding the online domain. Moreover, they are essential for achieving online security (Furnell, Jusoh, & Katsabas, 2006; Liang & Xue, 2010; Ng, Kankanhalli, & Xu, 2009).

The present study deals with the safety and security of online banking from an end-user perspective. Online banking is a means by which customers can access different kinds of banking services via the internet. By 2015, 85% of Dutch citizens of 16 years of age and over had adopted this service (Eurostat, 2016). However, as the internet also attracts criminals (Bossler & Holt, 2009; Van Wilsem, 2011b), online banking is not without risk. End users are, for example, confronted with phishing and malware attacks (Jansen & Leukfeldt, 2015) – techniques fraudsters use to obtain user credentials to steal money from their bank accounts. Because banks cannot control their customers' behaviour or the devices they use, it is important that end users are aware of threats aimed at online banking and are able to prevent them from manifesting in harm (Furnell & Clarke, 2012; Jansen, 2015). A challenge here is that although end users are ultimately responsible for their own online behaviour and the security of their devices, they often have insufficient knowledge or lack the tendency to protect themselves (Furnell, Tsaganidi, & Phippen, 2008) and are also not adequately aware of the online threats they are faced with (Kritzinger & Von Solms, 2010).

Furthermore, an international phenomenon regarding online banking is a shift in responsibility towards the end user (Anderson, 2007; Davinson & Sillence, 2014). On the one hand, this is not surprising because the safety and security of online banking cannot be addressed by banks alone. However, there is some debate on how far user responsibility should go, as online banking is a service that is pushed towards bank customers. It is not a voluntary choice in the sense

that traditional banking services are made more expensive and less accessible, for example, by closing local bank offices. Ultimately, a combination of technical, human and also legal aspects is required to ensure a safe online environment. To that extent, end users thus also have responsibilities regarding the safety and security of online banking. In this chapter, we study what motivates end users to protect themselves against online threats by analysing three social cognitive models. A better understanding of precautionary online behaviour is required to enhance safety and security from an end-user perspective.

The current study evaluates three models in terms of their effectiveness in explaining precautionary online behaviour.[39] We compare the protection motivation theory (PMT) (Maddux & Rogers, 1983; Rogers, 1975), the reasoned action approach (RAA) (Fishbein & Ajzen, 2010) and an integrated model which comprises PMT and RAA variables. Both PMT and RAA seem equally valuable in the present context and are discussed in more detail in Section 6.2. By testing individual and integrated models, we make two contributions: theoretical knowledge is advanced and maximum effectiveness is pursued (Lippke & Ziegelmann, 2008; Sommestad, Karlzén, & Hallberg, 2015). In addition, based upon Ifinedo's (2012) work, we expect the integrated model to provide a more comprehensive account of the determinants of precautionary online behaviour. Our main interest is aimed at explaining variance rather than assessing the quality of the models (Prochaska, Wright, & Velicer, 2008).

Both PMT and RAA (including RAA's predecessors) have been tested extensively to predict numerous behavioural intentions and actual behaviours. However, to the best of our knowledge, they have neither been widely compared in the information security domain nor extensively tested in an integrated fashion. Comparison is needed to help researchers make informed decisions about the usefulness of social cognitive models in this area. Therefore, the aim of our study is to evaluate the usefulness of PMT and RAA in explaining precautionary online behaviour. In addition, our study advances the understanding of precautionary online behaviour, which is still limited (Anderson & Agarwal, 2010; Liang & Xue, 2010; Ng et al., 2009). The results are useful for scholars and practitioners who want to study and improve online safety and security practices by end users in general, and safety and security in online banking in particular.

[39] In this chapter, precautionary online behaviour refers to the adherence to the safety rules of online banking and is operationalized as protection motivation, i.e., behavioural intentions. Note that these terms are used interchangeably.

6.2 Theory

In this section, first, an overview of PMT (Section 6.2.1) and RAA (Section 6.2.2) is presented, complemented with definitions of the predictor variables and a set of hypotheses that are tested in this study. This is followed by a discussion of precautionary online behavioural intention, the target behaviour of our study (Section 6.2.3).

6.2.1 Protection motivation theory

To date, several models exist that try to explain and predict behaviour (Floyd, Prentice-Dunn, & Rogers, 2000). In the information systems domain, extensive research is done on the adoption of technology. Examples of adoption theories include the technology acceptance model (Davis, 1989) and the unified theory of acceptance and use of technology (Venkatesh, Morris, Davis, & Davis, 2003). However, most of these studies focus on 'beneficial technologies', of which online banking can be considered an example. 'Protective technologies', which focus on preventing negative outcomes, are an under-studied subject in this area (Chenoweth, Minch, & Gattiker, 2009). Moreover, studies on precautionary online behaviour and on how such behaviour can be changed are scarce (Ng et al., 2009). As research has shown that significant difference exists between beneficial and protective technologies (Dinev & Hu, 2005), it seems that other theories than adoption theories might be more appropriate.

We believe that PMT provides an appropriate theoretical background for the current study. The reasons for this are: first, the theory has been successfully applied to understand and predict the use of numerous protective measures (Milne, Sheeran, & Orbell, 2000). Second, PMT has evolved over time into a powerful explanatory theory for precautionary behaviour (Floyd et al., 2000). Third, PMT includes the concept of risk, which is absent in adoption theories (Johnston & Warkentin, 2010). Another important argument in favour of PMT, or its variants (e.g., threat control model [Workman, Bommer, & Straub, 2008], technology threat avoidance theory [Liang & Xue, 2009] and fear appeals model [Johnston & Warkentin, 2010]), is that they have recently been applied to the information security domain (Boss, Galletta, Lowry, Moody, & Polak, 2015; Vance, Siponen, & Pahnila, 2012). These studies have shown that PMT provides a useful framework for predicting precautionary online behaviour. This has been demonstrated for both home-computer users (Anderson & Agarwal, 2010; Chenoweth et al., 2009; Crossler, 2010; Johnston & Warkentin, 2010; Lai, Li, & Hsieh, 2012; Liang & Xue, 2010) and end users who operate within an organisational context (Herath & Rao, 2009; Ifinedo, 2012; Lee & Larsen, 2009; Lee, 2011; Pahnila, Siponen, & Mahmood, 2007; Vance et al., 2012; Workman et al., 2008; Workman, Bommer, & Straub, 2009). We also considered an

alternative, yet similar, theory: the health belief model (HBM) (Rosenstock, Stretcher, & Becker, 1988). This has been applied to information security issues previously as well (Davinson & Sillence, 2010; Ng et al., 2009). A primary difference between HBM and PMT is that HBM consists of a set of variables that have an effect on behaviour, while PMT arranges its predictor variables in cognitive processes that individuals apply to evaluate threats and coping measures (Prentice-Dunn & Rogers, 1986; Weinstein, 1993). We therefore believe that the variables and processes included in PMT make this theory more suitable for improving our understanding of precautionary online behaviour than HBM. Finally, PMT is useful for developing interventions (Floyd et al., 2000), as it is viewed as a framework to develop and evaluate persuasive communications (Norman, Boer, & Seydel, 2005).

According to PMT, end users are motivated to protect themselves based on threat appraisal and coping appraisal processes, implying that end users first evaluate possible threats and then possible coping strategies. These evaluations determine users' protection motivation, in other words, their intention to proceed, continue or avoid a given behaviour (Floyd et al., 2000). 'Protection motivation is an intervening variable that has the typical characteristics of a motive: it arouses, sustains and directs activity' (Rogers, 1975, p. 98). Depending on the level of protection motivation aroused, end users will adopt an adaptive or maladaptive coping response. The former means that end users actually follow the recommended response, in this case, taking precautions. The latter holds that end users do not follow the recommended response, thereby potentially exposing themselves increasingly to online threats.

In PMT, the threat appraisal process consists of perceived vulnerability and perceived severity. Crossler (2010) describes perceived vulnerability as the personal probability or likelihood of a security incident occurring, and perceived severity as the impact of consequences resulting from a security incident. The rewards-construct is also part of PMT's threat appraisal process, but is often omitted (Milne et al., 2000) – also in our study – because the theoretical difference between a reward associated with not following the coping response and a response cost (part of the coping appraisal process) is in doubt (Abraham, Sheeran, Abrams, & Spears, 1994). Threat appraisal is a unique component in PMT that is not present in RAA. Based on the notions above, we can state our first two hypotheses as follows:

H1. Perceived vulnerability positively influences precautionary online behavioural intention.

H2. Perceived severity positively influences precautionary online behavioural intention.

The coping appraisal process includes an evaluation of the estimated coping strategies to avoid or minimise a threat. This process consists of response efficacy, self-efficacy and response costs. Milne et al. (2000) describe the first construct as the perceived effectiveness of a response in reducing a threat, the second as users' belief about whether they are capable of performing the recommended response and the third as how costly performing the response will be to the user. Notably, we use a domain-specific interpretation of self-efficacy as proposed by Rhee, Kim, and Ryu (2009, p. 818), who term this 'self-efficacy in information security' as: 'a belief in one's capability to protect information and information systems from unauthorised disclosure, modification, loss, destruction and lack of availability'. Thus, we arrive at our next hypotheses:

H3. Response efficacy positively influences precautionary online behavioural intention.

H4. Self-efficacy positively influences precautionary online behavioural intention.

H5. Response costs negatively influence precautionary online behavioural intention.

6.2.2 Reasoned action approach

Although specific theories are preferred when studying specific behaviour, more general theories for predicting human behaviour may contain variables that are important within the context that is being investigated. One such theory is RAA, which evolved from the popular theory of reasoned action (Fishbein & Ajzen, 1975) and the theory of planned behaviour (Ajzen, 1991). The essence of Fishbein and Ajzen's (2010) framework is that attitude towards behaviour, perceived norms and perceived behavioural control determine users' intention to perform a given behaviour. It is assumed that behavioural intention predicts actual behaviour. Moreover, they believe that their approach is unified, accounting for any behaviour. Therefore, their approach should also be appropriate for information security behaviour.

Attitude reflects a user's positive or negative feelings towards performing the target behaviour (Fishbein & Ajzen, 1975). A positive attitude towards certain behaviour is considered to positively influence that behaviour. An additional rationale for adopting this construct is that its relation with intentional behaviour has been extensively tested and corroborated (Venkatesh et al., 2003). Based on these notions, we arrive at our sixth hypothesis:

H6. A positive attitude positively influences precautionary online behavioural intention.

Perceived norms, unique in RAA compared to PMT, refer to perceived social pressure and are made up of injunctive norms – perceptions of what should or ought to be done – and descriptive norms – perceptions of whether others are performing the target behaviour (Fishbein & Ajzen, 2010). According to Anderson and Agarwal (2010), there has been a lack of attention to social variables in information systems research even though these variables are considered important for users' behaviour. Consequently, our next two hypotheses are as follows:

H7. Injunctive norms positively influence precautionary online behavioural intention.

H8. Descriptive norms positively influence precautionary online behavioural intention.

Fishbein and Ajzen (2010) describe perceived behavioural control as perceptions about being capable of or having control over the target behaviour. Perceived behavioural control is viewed as a combination of self-efficacy (also found in PMT, H4) and locus of control (Workman et al., 2008). Rather than selecting the single construct of perceived behavioural control, we have chosen to adopt these two constructs because they are distinct (Bandura, 1977). Locus of control is either internal or external (Rotter, 1966; Workman et al., 2008). End users who have a high level of internal locus of control believe that they are in control of the outcomes of a certain event. In this context, internal locus of control can translate into proactive behaviour by end users, taking responsibility for their online safety. End users who are characterized by external locus of control believe that the outcome is controlled by powerful others or by fate. This could translate into reactive behaviour, leaving responsibility to others – expectedly, their bank. This leads us to our final hypothesis:

H9. Internal locus of control positively influences precautionary online behavioural intention.

6.2.3 Precautionary online behaviour

The recommended actions that banks want their customers to take are found in the so-called uniform safety rules for online banking. These rules are defined in the general terms and conditions of all banks in The Netherlands and are in effect as of January 1, 2014. The items of the outcome variable of this study are based on these rules. The five rules for safe online banking comprise of the following: (a) keep your security codes secret; (b) make sure that your debit card is not used by others; (c) secure the devices you use for online banking properly; (d) check your bank account regularly; and (e) report incidents directly to your bank. In summary, precautionary online behaviour includes both technical and non-technical measures against security threats.

The dependent variable thus consists of items that refer to multiple actions. Although this approach is sometimes criticised (Blythe, Coventry, & Little, 2015) – because predictor variables might influence protection motivation for one behaviour, but not for another – others (Crossler & Bélanger, 2014) defend this approach, stating that precautionary behaviour against online threats constitutes taking multiple actions. Based on this notion and certain practical considerations (lack of validated scales for precautionary online behaviour and length of questionnaire), we chose to ask participants questions about their intentions to adhere to the uniform safety rules, as intentions are acknowledged to be the most immediate predictor of actual behaviour (Fishbein & Ajzen, 2010). Moreover, we followed the work of others in constructing the dependent variable, who also measured intentions that signified various actions (Anderson & Agarwal, 2010; Herath & Rao, 2009; Ifinedo, 2012). In conclusion, we justify our approach with our aim to gain insight into the safety and security intentions of end users, based on the totality of rules presented to them by Dutch banks.

6.3 Method

In this section, we describe the methods used to test the hypotheses and evaluate which model is most effective in predicting users' motivation for precautionary online behaviour. First, we discuss the survey questionnaire and procedure (Section 6.3.1). Second, we provide details on the survey participants (Section 6.3.2). We then discuss data analysis, validity and reliability of measures (Section 6.3.3).

6.3.1 Survey questionnaire and procedure

Based on literature study, using international databases – ACM Digital Library, ScienceDirect and Web of Science – we developed a questionnaire. We based the questionnaire items on the work of Anderson and Agarwal (2010), Herath and Rao (2009), Ifinedo (2012), Ng et al. (2009), Witte (1996) and Workman et al. (2008). The items used a five-point Likert-scale (ranging from totally disagree to totally agree), were translated in Dutch, programmed in LimeSurvey (an open-source online survey tool) and presented in random order. All predictor variables were measured by three items and precautionary online behaviour was measured by four items. Two examples of the items adopted are: 'the uniform safety rules help in preventing online banking fraud' (RE1) and 'it is my intention to comply with the uniform safety rules' (PM4). The full questionnaire is available in Appendix III. Before the participants were presented with these items, the uniform safety rules were explicitly defined, to ensure that participants have a common understanding of these rules as far as possible.

A draft version and an interactive online version of the questionnaire were pre-tested qualitatively by 12 individuals from the target population, major figures

from the banking sector and academic peers. Based on the results of pre-testing, some minor revisions – such as clarifying instructions and specifying terms and concepts – were made to the questionnaire. The interactive online version was also pre-tested quantitatively by 34 students. Some adjustments needed to be made regarding the wording of the items, since three scales showed low reliability (self-efficacy, response costs and locus of control). For the main study, participants were recruited by an external recruitment service of online survey panels. The questionnaire was online in May-June 2015.

6.3.2 Survey participants

In total, 1,200 Dutch users of online banking services completely filled out the online questionnaire. Participants' age ranged from 18 to 85 years (M = 49, *SD* = 14.5) and the gender distribution was 55% female and 45% male. Participants had completed at most: lower secondary education (15%), upper secondary education (32%) or higher education (53%) and were employed (54%), self-employed (7%), retired (19%) or had a different work status (20%) such as student and unemployed.

They were experienced internet users as more than half of the participants indicated that they having made use of it for over 15 years (53%) and about a third between 11-15 years (30%). One in 25 indicated as having used the internet for five years or less (4%) and one in eight for 6-10 years (13%). Besides online banking, they used the internet for various purposes, most notably for e-mail (98%), searching for information (90%), buying products or services (80%), reading news (79%) and social networking (66%). The majority of participants were frequently online, that is, more than 20 hours a week (39%) and between 10-20 hours a week (29%). About one in ten was less than 3 hours online per week (9%) and about a quarter between 3-10 hours (24%).

Participants were reasonably experienced users of online banking. The largest group had 6-10 years of experience with online banking (44%). About a third was more experienced, having used it for 11-15 years (22%) and over 15 years (12%). Just below 1% had less than a year's experience with online banking and 22% had 1-5 years of experience. Online banking is frequently used to check the account balance. About a quarter of participants did this on a daily basis (24%) and over a third on a weekly basis (38%). The remaining participants did this once every two weeks (18%), once a month (12%) and less than once a month (8%). Making payments via online banking was done less frequently. Most participants did this once every week (30%) or once every two weeks (35%). The remainder of the participants reported doing this daily (4%), monthly (23%) or less than once a month (8%).

6.3.3 Data analysis, validity and reliability

Partial least squares path modelling (PLS), using SmartPLS 2.0 (Ringle, Wende, & Will, 2005), has been used for data analysis. PLS can be described as a class of multivariate techniques to study relationships between measured variables and latent variables and relationships between latent variables (Hair, Hult, Ringle, & Sarstedt, 2014). PLS is compatible with multiple regression analysis, analysis of variance and unrelated *t*-tests, the results of which are special cases of the results of PLS, but which do not account for measurement error, while PLS does. As recommended by Henseler, Ringle, and Sinkovics (2009), we have used a standard bootstrapping procedure (N = 5,000) to test the significance of the model parameters.

Component loadings of the individual items, except one item of response costs (RC3) which was subsequently deleted, loaded highly (≥ .70) on the corresponding component, providing evidence for uni-dimensionality of the items. However, we had to remove two self-efficacy (SE1 and SE3) and attitude (AT2 and AT3) items, because these items loaded high on protection motivation as well (see Table 6.1). Therefore, both constructs have been represented by only one item in the structural models, posing a potential threat to reliability. We chose to retain these constructs since these are important components in PMT and RAA respectively. Construct reliability has been assessed using the composite reliability co-efficient; for all items, the cut-off point of .70 was exceeded (see Table 6.2).

Convergent validity was assessed using the average variance extracted (AVE) by a construct from its indicators, which for all, except for locus of control (.65), exceeded the cut-off point of .70. However, we chose to retain this construct as more variability in the items of locus of control was accounted for by its component than not. Discriminant validity was assessed by analysing the square root of AVE by each indicator's construct, which should be greater than its correlation with the remaining constructs (Fornell–Larcker criterion). All values met this condition (see Table 6.3). Additional SPSS analysis showed lack of multicollinearity.

Table 6.1: Component loadings – original measurement model (full)

	PV	PS	RE	SE	RC	IN	DN	AT	LoC	PM
PV1	**0.89**	0.17	-0.26	-0.24	0.24	0.17	-0.02	-0.15	-0.27	-0.17
PV2	**0.91**	0.22	-0.28	-0.28	0.28	0.22	0.02	-0.18	-0.29	-0.20
PV3	**0.72**	0.21	-0.17	-0.15	0.12	0.11	-0.01	-0.06	-0.20	-0.09
PS1	0.22	**0.86**	0.06	0.16	-0.04	0.04	0.12	0.24	0.07	0.22
PS2	0.13	**0.87**	0.11	0.25	-0.11	-0.05	0.09	0.31	0.09	0.28
PS3	0.26	**0.88**	0.05	0.14	0.01	0.07	0.11	0.25	0.03	0.21
RE1	-0.25	0.08	**0.89**	0.60	-0.32	0.00	0.33	0.65	0.59	0.64
RE2	-0.23	0.03	**0.77**	0.47	-0.17	0.08	0.28	0.54	0.56	0.48
RE3	-0.25	0.10	**0.88**	0.59	-0.33	-0.02	0.33	0.65	0.61	0.66
SE1	-0.24	0.19	0.58	**0.89**	-0.46	-0.13	0.21	0.64	0.54	0.71
SE2	-0.24	0.18	0.57	**0.87**	-0.42	-0.08	0.25	0.65	0.51	0.65
SE3	-0.24	0.20	0.61	**0.91**	-0.51	-0.10	0.30	0.67	0.58	0.75
RC1	0.23	-0.07	-0.29	-0.49	**0.90**	0.31	-0.02	-0.40	-0.31	-0.40
RC2	0.24	0.00	-0.25	-0.40	**0.85**	0.34	-0.02	-0.27	-0.23	-0.30
RC3	0.10	0.12	0.19	0.05	**0.14**	0.22	0.20	0.18	0.15	0.14
IN1	0.17	0.03	0.05	-0.05	0.25	**0.88**	0.20	-0.01	0.06	0.01
IN2	0.20	0.02	-0.02	-0.14	0.36	**0.87**	0.13	-0.06	-0.03	-0.09
IN3	0.17	0.02	0.03	-0.09	0.30	**0.90**	0.18	-0.05	0.03	-0.03
DN1	0.02	0.13	0.32	0.28	-0.06	0.12	**0.87**	0.29	0.27	0.31
DN2	0.00	0.09	0.30	0.20	0.00	0.19	**0.86**	0.27	0.29	0.29
DN3	-0.03	0.10	0.34	0.27	-0.04	0.19	**0.88**	0.30	0.30	0.33
AT1	-0.17	0.23	0.65	0.65	-0.37	-0.04	0.27	**0.87**	0.50	0.68
AT2	-0.11	0.30	0.64	0.63	-0.33	-0.02	0.34	**0.90**	0.51	0.75
AT3	-0.16	0.29	0.67	0.70	-0.38	-0.06	0.29	**0.92**	0.55	0.82
LoC1	-0.26	0.13	0.61	0.56	-0.30	-0.02	0.26	0.54	**0.83**	0.56
LoC2	-0.27	0.04	0.56	0.53	-0.25	0.03	0.28	0.46	**0.81**	0.49
LoC3	-0.17	0.02	0.52	0.39	-0.19	0.08	0.29	0.41	**0.77**	0.41
PM1	-0.14	0.22	0.58	0.66	-0.36	-0.03	0.32	0.71	0.49	**0.88**
PM2	-0.19	0.25	0.65	0.69	-0.36	-0.02	0.32	0.72	0.53	**0.90**
PM3	-0.18	0.26	0.64	0.76	-0.40	-0.04	0.34	0.73	0.56	**0.90**
PM4	-0.16	0.25	0.66	0.72	-0.39	-0.07	0.29	0.83	0.55	**0.90**

Note. PV: perceived vulnerability. PS: perceived severity. RE: response efficacy. SE: self-efficacy. RC: response costs. IN: injunctive norms. DN: descriptive norms. AT: attitude. LoC: locus of control. PM: protection motivation.

Table 6.2: Descriptives and coefficients of reliability and convergent validity

	Mean (M)	Standard deviation (*SD*)	Average variance extracted (AVE)	Composite Reliability (CR)
Perceived vulnerability	2.61	0.71	0.71	0.88
Perceived severity	3.96	0.76	0.76	0.90
Response efficacy	4.18	0.67	0.72	0.88
Self-efficacy	4.38	0.70	1.00	1.00
Response costs	2.12	0.86	0.77	0.87
Attitude	4.49	0.67	1.00	1.00
Injunctive norms	2.59	1.02	0.65	0.84
Descriptive norms	3.60	0.74	0.76	0.90
Locus of control	4.04	0.71	0.64	0.84
Protection motivation	4.38	0.64	0.80	0.94

Table 6.3: Coefficients of discriminant validity

	PV	PS	RE	SE	RC	AT	IN	DN	LoC	PM
PV	0.84									
PS	0.22	0.87								
RE	-0.29	0.09	0.85							
SE	-0.24	0.18	0.57	1.00						
RC	0.27	-0.05	-0.31	-0.40	0.88					
AT	-0.18	0.24	0.64	0.60	-0.36	1.00				
IN	0.21	0.02	-0.02	-0.10	0.38	-0.05	0.81			
DN	0.00	0.12	0.37	0.25	-0.03	0.27	0.14	0.87		
LoC	-0.30	0.09	0.70	0.52	-0.30	0.51	-0.01	0.34	0.80	
PM	-0.19	0.28	0.71	0.65	-0.40	0.68	-0.09	0.36	0.61	0.89

Note. Off-diagonal values are correlations. Diagonal values are square root of average extracted variances. PV: perceived vulnerability. PS: perceived severity. RE: response efficacy. SE: self-efficacy. RC: response costs. AT: attitude. IN: injunctive norms. DN: descriptive norms. LoC: locus of control. PM: protection motivation.

6.4 Results

The structural models with the test results are presented in Figures 6.1-6.3. The asterisks indicate a significance level of $p < .001$ and 'ns' stands for not significant. We evaluated the significance of the model predictors of precautionary online behaviour.

In total, 64% of variance in precautionary online behaviour is explained by PMT's predictors perceived vulnerability, perceived severity, response efficacy, self-efficacy and response costs (Figure 6.1). The strongest positive predictor is response efficacy, followed by self-efficacy and perceived severity and the negative predictor response costs. Perceived vulnerability has no significant effect on precautionary online behaviour.

Further, 63% of variance in precautionary online behaviour is explained by RAA's predictors attitude, injunctive norms, descriptive norms, self-efficacy and locus of control (Figure 6.2). The strongest positive predictor is attitude, followed by self-efficacy, locus of control (internal) and descriptive norms. Injunctive norms have no significant effect on precautionary online behaviour.

In addition to evaluating the explained variance of both structural models, we also calculated the effect size. According to Hair et al. (2014), this provides information on how substantive the impact is of both the models. In terms of the effect size f^2, the additional variance explained by PMT over and above RAA ($f^2 = .16$) and the additional variance explained by RAA over and above PMT ($f^2 = .13$), both represent an approximately medium effect ($f^2 = .15$ [Hair et al., 2014]).

Figure 6.1: Structural model PMT variables

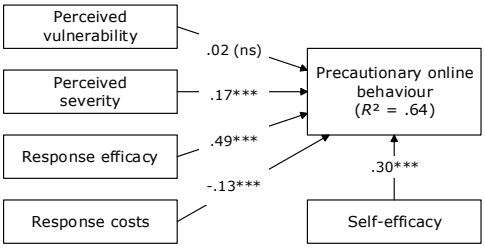
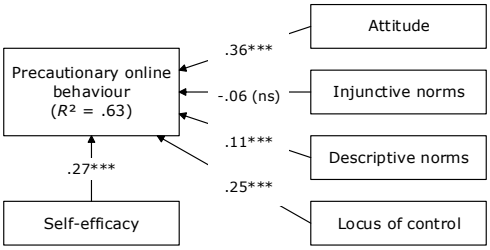
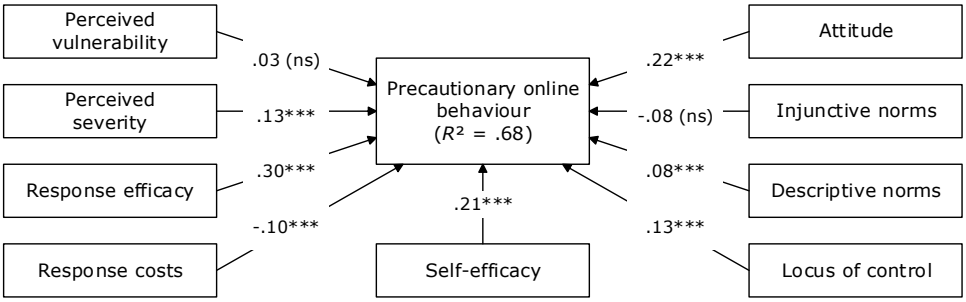


Figure 6.2: Structural model RAA variables



In the integrated model, explained variance of 68% is highest (Figure 6.3). The PMT variables perceived severity, response efficacy and response costs, the RAA variables attitude, descriptive norms and locus of control, and self-efficacy from both models are significant predictors of precautionary online behaviour (see Figures 6.1-6.3). Therefore, all hypotheses are accepted, except for H1 and H7 – thus, perceived vulnerability and injunctive norms are not significant predictors.

Figure 6.3: Structural model PMT-RAA variables



6.5 Conclusion and discussion

Our study has some limitations. First, the attitude construct contains one item only for hypotheses-testing, which potentially threatens reliability. Only three items were included in the questionnaire to measure this rather complex construct. Although the scale itself was reliable, two items loaded too heavily on protection motivation. Future research could make use of a more robust measure of attitude, as its explanatory power is often shown (Ifinedo, 2012, 2014; Venkatesh et al., 2003). However, Herath and Rao (2009) found no significant relationship between attitude and security policy compliance. They attributed this result to factors such as context, sample and other extraneous factors. Furthermore, they argue that the predictive power of attitude might be reduced by the inclusion of other constructs, such as self-efficacy and norms. Hence, the precise effect of attitude in this regard is an interesting topic for future research.

A second limitation can be attributed to the self-efficacy construct, which is represented by only one item for hypotheses-testing as well, also possibly threatening reliability. Similar to the attitude scale, the self-efficacy scale itself was reliable, but again two items loaded too heavily on protection motivation. Future research needs to address this limitation by using a more robust measure. Specifically, multiple-item measures lead towards higher predictive validity (Hair et al., 2014), which could mean that self-efficacy could be an even a stronger predictor than it already is.

Third, we relied on self-reported behavioural intention, which could be considered a limitation. Therefore, we recommend observing actual behaviour in future studies, particularly to overcome the intention-behaviour gap (see also Boss et al.'s [2015] commentary on PMT studies and Crossler et al.'s [2013] agenda for future behavioural information security research).

The aim of our study was to evaluate the usefulness of PMT and RAA in explaining precautionary online behaviour. PMT and RAA both show good explanatory power, which indicates that both seem valuable in explaining this kind of behaviour. A main contribution of the combined model is that it shows that the individual predictors of the two constituent models (PMT and RAA) remain significant, thereby potentially providing practitioners more opportunities for prevention through increasing people's precautionary behaviour. Significant predictors should, for example, be emphasised in prevention campaigns in an effort to achieve behavioural change. Increased precautionary behaviour of end users is beneficial for banks, as it might reduce the number of online banking fraud incidents.

Among the predictor variables of PMT, response efficacy and self-efficacy are most important. This means that the more effective a measure is perceived to be and the better the perceived ability of carrying out a measure, the more likely precautionary behaviour is, which concurs with previous studies (Crossler, 2010; Ifinedo, 2012; Lee, 2011; Liang & Xue, 2010; Workman et al., 2008). In contrast to Sommestad et al.'s (2015) findings, our results show that coping response (from PMT) is significant in explaining variance. Attitude, from RAA, can also be considered a primary predictor variable. The more positive the attitude towards precautionary online behaviour, the more likely such behaviour is, which has also been demonstrated in earlier studies (Anderson & Agarwal, 2010; Fishbein & Ajzen, 2010; Venkatesh et al., 2003). Scholars and practitioners should acknowledge these primary variables when developing prevention campaigns.

Secondary determinants of explaining precautionary online behaviour, which behave in accordance with literature, are: perceived severity (Chenoweth et al., 2009; Gurung, Luo, & Liao, 2009; Lee, 2011; Vance et al., 2012; Workman et al., 2008) and locus of control (Ifinedo, 2014; Workman et al., 2008). If end users evaluate the impact of a threat as high and believe that threat prevention is something they are in control of (internal locus of control), they will be more likely to adopt a recommended coping measure. Therefore, these variables should also be considered when implementing prevention strategies. Moreover, underscoring personal responsibility is found to be an important aspect in stimulating protection motivation (Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015; Shillair et al., 2015).

The final two constructs that are significant predictors of protection motivation are: the negative predictor response costs and the positive predictor descriptive norms. Both are in the proposed direction, as was expected based on literature (Chenoweth et al., 2009; Herath & Rao, 2009; Lee, 2011; Liang & Xue, 2010; Vance et al., 2012). This means that when end users consider the costs of a measure as not outweighing its benefits and believe that others are taking precautions, they are likely to (also) perform precautionary online behaviour. The former is important for banks, as this means that they should find a favourable balance between the usability of their services and the tangible and intangible costs of precautionary measures. The latter could, for example, be achieved by showing in prevention campaigns how others are taking precautionary measures.

Perceived vulnerability has no significant effect on protection motivation. Earlier studies found mixed results for this construct. Gurung et al. (2009) and Vance et al. (2012) also reported a non-significant relationship. However, Chenoweth et al. (2009), Lee (2011) and Workman et al. (2008) found a positive relationship between perceived vulnerability and protection motivation. Crossler's (2010) study on the other hand, revealed a negative relationship. He explains that different outcomes can be attributed to the specific threats and behaviours studied and that future research is necessary to determine its true relationship.

Injunctive norms are non-significant as well, contradicting earlier studies (Herath & Rao, 2009; Ifinedo, 2012, 2014). However, contrary to our study, these studies took place in organisations, while security of online banking may be seen as an individual rather than a social issue. It is probably not a subject that is often addressed in social conversations.

Although there seems to be overlap between the models, it is important to stress that theory is advanced by testing the usefulness of these theories in the

study of online behaviours. However, considering the advancement of theory, Ogden (2003) argues that this is problematic due to the unspecific nature of the constructs involved. Indeed, though the scales we used and the relationships we found were predetermined based on theory, the questionnaire items needed to be specified to the online domain in general and specifically to the online banking context. Another problem Ogden (2003) identifies is that social cognitive models often rely on analytic truths instead of synthetic truths. Qualitative exploratory research is recommended to identify predictor variables that are accountable for the variance we were not able to explain.

For now, it seems that the integrated model is most effective in explaining variance. This conclusion is consistent with the work of Herath and Rao (2009) and Ifinedo (2012). However, as explained by Lippke and Ziegelmann (2008), one theory can be more suitable for explaining a specific behaviour across populations and another for explaining diverse behaviours in a specific population. It is uncertain to what extent the results are generalizable to other countries, since different countries have different payment cultures. For example, the uptake of online banking is high in The Netherlands and Nordic countries as compared to other European countries (Eurostat, 2016). Additionally, other cultural differences, such as uncertainty avoidance and power distance – both within and between countries – could have an influence on precautionary online behaviour (Crossler et al., 2013). Besides, the political and economic situation of a country (Aldás-Manzano, Lassala-Navarré, Ruiz-Mafé, & Sanz-Blas, 2009) could also have an impact, for example, on risk perceptions. Future research is needed – across different domains, behaviours and populations – to advance our knowledge in behavioural information security and to understand which of these (or competing) models best explains precautionary online behaviour of end users.

In conclusion, our recommendations for enhancing precautionary online behaviour should be tested in practice. A fruitful way forward might be using experimental manipulations of PMT and RAA variables, as recommended by Shillair et al. (2015), to find the most promising strategies. To our knowledge, studies that investigate the power of either model's predictors to create preventative measures are lacking. Additionally, future studies could benefit from including measurement of fear and the effect of using fear appeal manipulations to enhance such strategies (Boss et al., 2015). Furthermore, it is important to find out how and how often end users should be presented with such information, to most effectively promote precautionary online behaviour.

CHAPTER 7

Testing a model of precautionary online behaviour: The case of online banking

Jurjen Jansen

Paul van Schaik

Submitted.

7.1 Introduction

As networked technology becomes increasing pervasive in our world, the burdens and responsibilities of people who use networked technology rise. Individuals need to protect their confidential information, such as passwords and credentials used for online banking services. Once third parties get a hold of such information, they can take over people's (online) identities and access their online bank accounts. This is undesirable since it can seriously damage people's lives and lower their level of trust in online financial transactions, which are essential in our economy. However, behaving safe online and being adequately protected against online threats is not easy.

Technology alone is unable to protect people against online threats, which makes human behaviour of crucial importance (Furnell, Jusoh, & Katsabas, 2006; Liang & Xue, 2010; Ng, Kankanhalli, & Xu, 2009; Rhee, Kim, & Ryu, 2009). Although people are often referred to as the weakest link in information security (Moore & Anderson, 2011) they can play an essential role in safeguarding information. According to Huang, Rau, and Salvendy (2010), it becomes increasingly clear that the human factor is the Achilles heel of information security. Therefore, a socio-technical or behavioural approach to security seems desirable (Anderson & Agarwal, 2010).

This study focusses on the safety and security of a particular online service, namely online banking. With online banking, users have access to various banking services via the internet, such as viewing account balances and paying bills. Users can access their bank accounts online through a graphical user-interface – facilitated by a web browser or app – on a device selected by the customer, such as PC, laptop, smartphone and tablet.

Banks cannot control customer behaviour nor the devices customers use for online banking. This means that customers themselves have certain responsibilities regarding the safety and security of online banking. Moreover, customers' behaviour is often the cause for online banking fraud victimization (Jansen & Leukfeldt, 2015). Consequently, customers should be able to cope with threats aimed at online banking. Therefore, customers should be aware of threats, try to prevent them, and when a threat manifests itself recognize it and act accordingly (Jansen, 2015). One way of preventing threats is taking precautionary measures. The question relevant to this study is how online banking customers can be motivated to take such measures. A better understanding of user motivations is required to enhance safe online banking behaviour.

The aim of our study is to gain insight into factors that influence customers to take measures to protect themselves against online threats. We do this by developing a research model and then testing this. The threat central to our study is online banking fraud, which can be established in different ways, for example by phishing and malware attacks. The commonality is that a security incident occurred that involves the deception of a customer or a system used for online banking in order to obtain user-credentials and/or to gain control over a customer's device which can be used by criminals for financial gain (Jansen & Leukfeldt, 2016).

This study contributes to a better understanding of precautionary behaviour by customers of online banking.[40] Precautionary or safe behaviour includes both technical measures and behavioural measures related to computer and internet usage, such as anti-virus software and conscious care behaviour (Rhee et al., 2009). Research in this area is still limited (Anderson & Agarwal, 2010; Liang & Xue, 2010), also with regard to behavioural change (Anderson & Agarwal, 2010; Ng et al., 2009). Moreover, little is known about security awareness and security behaviours of end-users using technology for financial transactions (Davinson & Sillence, 2014). The results can be used by scholars and practitioners when designing security education, training and awareness campaigns aimed at safe online banking, thereby empowering online banking customers to better protect themselves against online threats.

Our study includes various unique features. First, our model includes the concept of trust. Second, unlike other similar models, the model we propose has not yet been applied to the context of online banking. Third, this study benefits from a large dataset of the Dutch population. Fourth, we test the model on different subgroups, which is often neglected in online-security research, but is recommended to further differentiate the findings by demographics (Hair, Hult, Ringle, & Sarstedt, 2014). Indeed, this is a major topic in behavioural research, for example in marketing (Blackwell, Miniard, & Engel, 2001), but is also important in online security. Specifically, a practical reason for investigating demographic differences is that it could be particularly meaningful in that it sheds some light on how to raise precautionary online behaviour for different kinds of people. It could also provide opportunities to better understand which groups of people to target regarding online threats and preventive measures.

[40] In this chapter, precautionary online behaviour refers to the adherence to the safety rules of online banking and is operationalized as protection motivation, i.e., behavioural intentions. Note that these terms are used interchangeably.

Note that this study builds on existing research of Jansen and Van Schaik (2017) who evaluated protection motivation theory, the reasoned action approach and a combination of the two on their effectiveness of explaining precautionary online behavioural intentions in the domain of online banking. And also partly on the work of Jansen, Kop, and Stol (2017) who studied end-user perceptions of the safety and security of online banking.

7.2 Theory

The current study uses protection motivation theory (henceforth PMT) as a basis for developing our research model. PMT (Maddux & Rogers, 1983; Rogers, 1975) is a social-cognitive model that predicts behaviour and is often used in health-related research, trying to predict and explain detection and prevention behaviour (Milne, Sheeran, & Orbell, 2000). Although the original purpose of PMT is to clarify fear appeals, it has since been adopted as a more general model to study decisions related to risk (Maddux & Rogers, 1983). After several modifications, PMT has become one of the best explanatory theories for predicting one's intention for protective behaviour (Floyd, Prentice-Dunn, & Rogers, 2000).

PMT has increasingly gained attention in information security research (Boss, Galletta, Lowry, Moody, & Polak, 2015; Vance, Siponen, & Pahnila, 2012). It provides a good foundation for studies within this area of study (Herath & Rao, 2009; Liang & Xue, 2009) and is deemed applicable in the domain of online banking (Jansen, 2015). The focus of earlier studies who adopted PMT ranges from compliance with information systems security policy (Herath & Rao, 2009; Ifinedo, 2012, 2014; Vance et al., 2012) to the adoption of anti-spyware software (Chenoweth, Minch, & Gattiker, 2009; Gurung, Luo, & Liao, 2009; Johnston & Warkentin, 2010; Liang & Xue, 2010) and from backing up data (Crossler, 2010) to protective behaviour towards identity theft (Lai, Li, & Hsieh, 2012).

According to PMT, two cognitive processes take a central place; threat appraisal and coping appraisal, which both influence protection motivation, the outcome variable of PMT. Threat appraisal process is performed initially (Floyd et al., 2000; Liang & Xue, 2009), in which an individual evaluates the likelihood and impact of a threat. Customers need to be aware of a threat first and assess this accordingly. Thereafter, coping appraisal process starts, in which an individual evaluates possible coping strategies aimed at lowering and/or mitigating the threat.

7.2.1 Precautionary behaviour

In PMT, the outcome variable is the intention to proceed, continue or avoid certain behaviour (Floyd et al., 2000). Taking precautionary measures aimed at safe online banking is the subject of the current study.

7.2.2 Threat appraisal

In the threat appraisal process, a user evaluates the level of danger linked to a security event (Crossler, 2010). Following the work of Liang and Xue (2010), this process is constituted by perceived risk, which in turn is influenced by perceived vulnerability and perceived severity. We have added trust in online banking as another predictor of perceived risk, as it might improve explanatory power of the model. Indeed, Yousafzai, Foxall, and Pallister (2010) demonstrated the importance of trust in understanding online banking behaviour.

Perceived risk. Perceived risk, in the case of online banking, is the perceived potential of loss as a consequence of using the service (Yousafzai, Pallister, & Foxall, 2003). Individuals will change their behaviour based on how much risk they are willing to take that is associated with a certain action (Workman, Bommer, & Straub, 2008). Specifically,

H1. Perceived risk positively influences precautionary online behaviour.

Perceived vulnerability. Perceived vulnerability is a user's evaluation of the probability that a threatening security event will happen to them (Crossler, 2010). In this case, the extent to which a customer believes that he will be victimized by online banking fraud. According to PMT, perceived vulnerability is a direct predictor of protection motivation as well. Consequently,

H2a. Perceived vulnerability positively influences perceived risk.

H2b. Perceived vulnerability positively influences precautionary online behaviour.

Perceived severity. Perceived severity is a user's evaluation of the severity of the consequences of a threatening security event happening to them (Crossler, 2010). In this case, the perceived seriousness of consequences due to online banking fraud. According to PMT, perceived severity is also a direct predictor of protection motivation. Hence,

H3a. Perceived severity positively influences perceived risk.

H3b. Perceived severity positively influences precautionary online behaviour.

Trust in online banking. Trust in online banking is 'a psychological state which leads to the willingness of customers to perform banking transactions on the internet, expecting that the bank will fulfil its obligations, irrespective of customer's ability to monitor or control bank's actions' (Yousafzai et al., 2003, p. 849). Studies into online banking adoption have shown that perceived risk is lowered when an individual possesses a higher level of trust (Davinson & Sillence, 2014; Yousafzai, Pallister, & Foxall, 2009). However, too much trust can lead to over-confidence and over-confidence may, according to Furnell (2008a), result in careless behaviour. Thus,

H4a. Trust in online banking negatively influences perceived risk.

H4b. Trust in online banking negatively influences precautionary online behaviour.

7.2.3 Coping appraisal

In the coping appraisal process, a user evaluates a given coping strategy to mitigate or avert a threatening security event (Crossler, 2010). According to PMT, this process encompasses response efficacy, self-efficacy and response costs. Based on existing behavioural research in information security, we have added three variables to the coping appraisal process: locus of control, injunctive norms and descriptive norms.

Response efficacy. Response efficacy is the perceived effectiveness of a coping response in reducing a threat (Milne et al., 2000). Our assumption is that if individuals are sufficiently convinced that a precaution will work, they are more likely to take it. Consequently, according to PMT,

H5. Response efficacy positively influences precautionary online behaviour.

Self-efficacy. We adopt the definition of Rhee et al. (2009) of self-efficacy in information security which is a user's belief in being capable to protect his information and information systems. Individuals who believe they are able to take certain precautions are more inclined to take such precautions as compared with individuals who have less confidence in themselves (see also Bandura [1977]). Therefore, according to PMT,

H6. Self-efficacy positively influences precautionary online behaviour.

Response costs. Response costs are a user's beliefs about how costly performing the coping response will be to the them (Milne et al., 2000). According to Crossler (2010), countermeasures are not taken when the costs, both tangible and intangible, outweigh the loss of a particular threat. Thus, according to PMT,

H7. Response costs negatively influences precautionary online behaviour.

Locus of control. Whereas the emphasis of self-efficacy is on whether individuals feel they have the right skills and capabilities to achieve a goal, locus of control comprises a more interactive expression of the relationship between an individual and his or her environment (Tu & Yuan, 2012; Workman et al., 2008). According to Workman et al. (2008), this construct – which they see as part of the coping appraisal process – influences whether individuals take responsibility themselves (internal locus of control), in this case taking precautionary measures, or leave responsibility to another entity (external locus of control), in this case their bank. Based on these notions,

H8. Internal locus of control positively influences precautionary online behaviour.

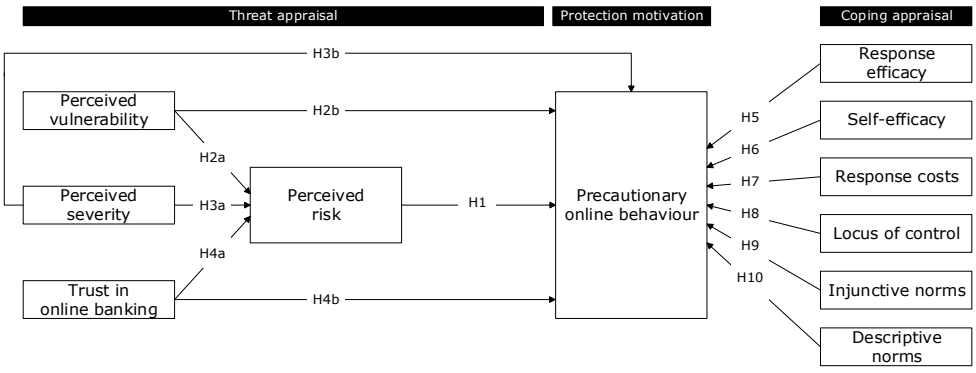
Norms. Anderson and Agarwal (2010) stress the importance of studying norms as a predictor of security behaviour. In order to acknowledge this issue, we include the constructs of injunctive norms and descriptive norms in our study and place them – like Ifinedo (2012) – within the coping appraisal process. Injunctive norms are perceptions regarding what should or ought to be done, whereas descriptive norms are perceptions whether others are or are not performing the target behaviour (Fishbein & Ajzen, 2010). Therefore,

H9. Injunctive norms positively influence precautionary online behaviour.

H10. Descriptive norms positively influence precautionary online behaviour.

Based on the discussion above, the research model is presented in Figure 7.1. Incorporating all hypotheses, we expect protection motivation to be a positive function of perceived risk, perceived vulnerability, perceived severity, response efficacy, self-efficacy, locus of control, injunctive norms and descriptive norms, and a negative function of trust in online banking and response costs. Similarly, we expect perceived risk to be a positive function of perceived vulnerability and perceived severity and a negative function of trust in online banking.

Figure 7.1: Research model



7.3 Method

7.3.1 Design

A survey design was used with outcome variables risk perception and protection motivation. The predictors included both variables from existing theory, in particular protection motivation theory, namely perceived vulnerability, perceived severity, response efficacy, self-efficacy, and response costs, and the reasoned action approach (Fishbein & Ajzen, 2010), namely injunctive norms and descriptive norms, as well as demographic variables that could be influential on protection motivation.

7.3.2 Participants

Sampling was done by an external recruitment service of online survey panels. They first sent out an invitation e-mail, including a hyperlink to the questionnaire, to a small batch of respondents. This was done to check whether the invitation and survey systems were appropriately linked. Thereafter, two larger batches were sent out in order to achieve a full response of 1,200 respondents. The aim was to achieve a representative sample of the Dutch population by means of stratified random sampling (by gender and age). As an incentive for their voluntary participation, the research participants received panel points that can be used for discounts at web shops or for donations to charities.

In total, 1,850 people visited the online questionnaire. The responses of 36 people were filtered out by the first question, because they did not belong to the target group; 14 mentioned to have online banking managed by someone else and 22 did not make use of online banking services at all. Finally, 614 did not (completely) fill in the questionnaire and were therefore excluded from the analysis. We were unable to obtain any additional information on the background characteristics of these people. The data were gathered in the months May and June of 2015.

The data of 1,200 Dutch citizens who used online banking were analysed (658 female, 542 male; mean age = 49.02, *SD* = 14.53). Respondents had completed primary or lower secondary education (15%), upper secondary education (32%) or higher education (53%). They were self-employed (7%), employed (54%), retired (19%), or had a different (work) status (20%), such as student, homemaker or unemployed. Seven in ten respondents considered themselves experienced users of online banking (70%) whereas one in eight did not (14%). The remainder of the respondents had a neutral opinion on their self-assessed experience (16%).

7.3.3 Survey questionnaire and procedure

In order to develop the questionnaire, a literature study was performed, using the following international databases of scientific publications: ACM Digital Library, ScienceDirect, and Web of Science. Moreover, a search for relevant literature was performed in reference lists of useful articles. For the development of the questionnaire we were particularly interested in validated scales. The scales that we used and the sources we based them on can be found in Appendix III.

The operationalization of the dependent variable provided a challenge, since there is no validated scale for safe online banking behaviour. For this study, we chose to base the dependent variable items on the so-called uniform safety rules for online banking, which are included in the General Terms and Conditions of all Dutch banks since the beginning of 2014. Before the respondents were presented with items to measure the dependent and independent variables, the safety rules were explicitly defined, to allow respondents to develop a common understanding of these rules. The five rules are (a) keep your security codes secret; (b) make sure that your debit card is not used by others; (c) secure the devices you use for online banking properly; (d) check your bank account regularly; and (e) report incidents directly to your bank.

The items of the outcome variable thus represent multiple actions. Crossler and Bélanger (2014) argue, however, that this is not a concern, considering that precautionary behaviour against threats constitutes taking multiple actions. Moreover, we believe that this approach is justified by our aim to gain insight into users' motivations for taking protective measures considering the safety and security of online banking, based on the totality of the safety advice given to them by the banks. In addition, we chose to refer to these rules, since they are relevant for Dutch online banking.

Individuals can choose to adhere to the safety rules (i.e., adaptive response), potentially protecting themselves to threats associated with online banking or to neglect them (i.e., maladaptive response), leaving themselves potentially vulnerable. Respondents were asked to answer questions about their intentions to adhere to the five uniform safety rules. Intentions are presumed to be the most immediate predictor of actual behaviour (Fishbein & Ajzen, 2010). In line with this reasoning, it is worthwhile to study people's behavioural intentions, since influencing behaviour can be accomplished by influencing people's intentions (O'Keefe, 2016). We adapted the scales from Anderson and Agarwal (2010), Herath and Rao (2009) and Ifinedo (2012), whose operationalisation of the intention measure also represented multiple actions.

The items of the pre-existing scales were applied to the current context and translated to Dutch, since the questionnaire needed to be filled in by Dutch respondents. The items of the constructs were presented in random order and used a 5-point Likert-scale, ranging from totally disagree to totally agree. The questionnaire was qualitatively pretested by the target group, academic peers and key informants from the banking sector (N = 9). After the required changes had been made, the questionnaire was programmed in LimeSurvey, an open-source online survey tool. Examples of changes include making the instructions clearer, simplifying use of language and specifying terms and concepts. The online version of the questionnaire was also qualitatively pretested by academic peers and key informants from the banking sector (N = 5) and then quantitatively by 34 students, primarily to check scale reliability and completion time, leading to minor adjustments. Four scales were adjusted (trust, self-efficacy, response costs and locus of control), mainly in wording, because they showed low reliability.

We have addressed potential common method bias in several ways (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). First, anonymity was guaranteed in the instructions to reduce the likelihood of social desirability in the answers of the participants. Second, we instructed the participants that there are no right or wrong answers. In addition, we tested our data by performing Harman's single-factor test which indicated that common method bias was not a problem.

7.3.4 Data analysis

Partial-least-squares path-modelling – PLS for short – was used for data analysis using SmartPLS 2.0 (Ringle, Wende, & Will, 2005). PLS was chosen over covariance-based structural equation modelling (henceforth CBSEM) because of the exploratory nature of the current study focussing on theory building and the predictive application instead of theory testing or confirmation (Barroso, Carrión, & Roldán, 2010; Hair et al., 2014). In addition, PLS does not require some of the assumptions imposed by CBSEM – including those of large sample size, and univariate and multivariate normality. Recent simulation studies have demonstrated that PLS performs at least as well as and, under various conditions, is superior to CBSEM in terms of bias, root mean square error and mean absolute deviation (Hulland, Ryan, & Rayner, 2010; Vilares, Almeida, & Coelho, 2010). In the analyses, a standard PLS bootstrapping procedure (N = 5,000, as Henseler, Ringle, and Sinkovics [2009] recommend) was used to test the significance of model parameters.

7.4 Results

We start by analysing the psychometric properties of the measurement instruments. We then analyse the structural model.

7.4.1 Measurement Model

Because of high cross-loadings with protection motivation, the items Self-efficacy 1 and Self-efficacy 3 were removed. The item Response Costs 3 was also removed since it loaded low on the factor response costs (see Appendix III). Component loadings of the final measurement model are presented in Table 7.1. Each item loaded highly on its corresponding component and considerably

Table 7.1: Component loadings – final measurement model

	PV	PS	PR	TR	RE	SE	RC	IN	DN	LoC	PM
PV1	**0.89**	0.17	0.63	-0.33	-0.26	-0.21	0.24	0.17	-0.02	-0.26	-0.17
PV2	**0.91**	0.22	0.69	-0.35	-0.28	-0.24	0.28	0.22	0.02	-0.28	-0.20
PV3	**0.73**	0.21	0.55	-0.24	-0.17	-0.14	0.12	0.11	-0.01	-0.19	-0.09
PS1	0.22	**0.87**	0.27	-0.08	0.06	0.13	-0.03	0.04	0.12	0.08	0.22
PS2	0.13	**0.86**	0.20	-0.03	0.11	0.22	-0.10	-0.05	0.09	0.10	0.28
PS3	0.26	**0.89**	0.37	-0.12	0.05	0.12	0.03	0.07	0.11	0.04	0.21
PR1	0.60	0.31	**0.85**	-0.38	-0.23	-0.18	0.28	0.21	0.05	-0.22	-0.09
PR2	0.68	0.22	**0.81**	-0.36	-0.32	-0.22	0.26	0.16	-0.03	-0.28	-0.20
PR3	0.61	0.30	**0.87**	-0.40	-0.26	-0.22	0.26	0.16	0.01	-0.29	-0.13
TR1	-0.35	-0.12	-0.45	**0.90**	0.40	0.24	-0.19	-0.02	0.15	0.41	0.24
TR2	-0.26	-0.01	-0.29	**0.82**	0.43	0.24	-0.18	0.01	0.22	0.45	0.29
TR3	-0.33	-0.10	-0.41	**0.83**	0.36	0.19	-0.14	0.01	0.16	0.35	0.19
RE1	-0.25	0.08	-0.29	0.39	**0.88**	0.48	-0.30	0.01	0.33	0.60	0.64
RE2	-0.23	0.03	-0.24	0.43	**0.77**	0.48	-0.15	0.08	0.28	0.57	0.48
RE3	-0.25	0.10	-0.28	0.36	**0.88**	0.49	-0.31	-0.02	0.33	0.62	0.66
SE2	-0.24	0.17	-0.24	0.26	0.57	**1.00**	-0.40	-0.08	0.25	0.52	0.65
RC1	0.23	-0.07	0.25	-0.19	-0.29	-0.38	**0.90**	0.31	-0.02	-0.30	-0.40
RC2	0.24	0.01	0.30	-0.17	-0.25	-0.33	**0.87**	0.33	-0.02	-0.22	-0.30
IN1	0.17	0.03	0.16	0.01	0.05	-0.03	0.27	**0.89**	0.21	0.07	0.01
IN2	0.20	0.03	0.22	-0.02	-0.02	-0.09	0.37	**0.86**	0.13	-0.02	-0.09
IN3	0.17	0.02	0.16	0.01	0.03	-0.07	0.31	**0.90**	0.19	0.04	-0.03
DN1	0.02	0.13	0.04	0.18	0.32	0.23	-0.05	0.13	**0.87**	0.28	0.31
DN2	0.00	0.10	0.02	0.17	0.30	0.19	0.01	0.19	**0.86**	0.30	0.29
DN3	-0.03	0.10	-0.03	0.19	0.34	0.23	-0.03	0.19	**0.88**	0.31	0.33
LoC1	-0.26	0.13	-0.27	0.41	0.61	0.45	-0.29	-0.02	0.26	**0.83**	0.56
LoC2	-0.27	0.04	-0.28	0.39	0.56	0.46	-0.23	0.03	0.28	**0.81**	0.49
LoC3	-0.17	0.02	-0.20	0.35	0.52	0.32	-0.18	0.08	0.29	**0.77**	0.41
PM1	-0.14	0.21	-0.12	0.22	0.58	0.57	-0.34	-0.03	0.32	0.50	**0.88**
PM2	-0.19	0.25	-0.16	0.26	0.65	0.56	-0.34	-0.02	0.32	0.54	**0.90**
PM3	-0.18	0.26	-0.15	0.26	0.64	0.61	-0.39	-0.04	0.34	0.57	**0.90**
PM4	-0.16	0.25	-0.16	0.26	0.66	0.60	-0.37	-0.07	0.29	0.57	**0.89**

Note. PV: perceived vulnerability. PS: perceived severity.PR: perceived risk. TR: trust. RE: response efficacy. SE: self-efficacy. RC: response costs. IN: injunctive norms. DN: descriptive norms. LoC: locus of control. PM: protection motivation.

lower on the remaining components, thereby providing evidence for unidimensionality of the items. Although self-efficacy is represented by one item, we retained this construct, because it is an important component in PMT.

In testing the measurement model, reliability was analysed (Table 7.2), and convergent and discriminant validity were assessed (Table 7.3). The reliability of each individual reflective item is assessed by its loading on the construct of which it is an indicator, which should be 0.70 or higher (Henseler et al., 2009). All loadings met this condition and were statistically significant, $p < .001$. At the construct level, reliability was analysed using the composite-reliability co-efficient, which needs to be 0.70 or higher. All the co-efficients exceeded this cut-off point.

Table 7.2: Coefficients of reliability and convergent validity

	Loading	AVE	CR	SE	t^a
Perceived vulnerability		0.71	0.88		
- PV1	0.89			0.01	87.05
- PV2	0.91			0.01	158.63
- PV3	0.73			0.02	36.75
Perceived severity		0.76	0.90		
- PS1	0.87			0.01	70.69
- PS2	0.86			0.02	51.30
- PS3	0.89			0.01	85.07
Perceived risk		0.72	0.88		
- PR1	0.85			0.01	77.50
- PR2	0.81			0.01	58.27
- PR3	0.87			0.01	105.50
Trust		0.72	0.89		
- TR1	0.90			0.01	94.52
- TR2	0.82			0.01	56.77
- TR3	0.83			0.02	52.36
Response efficacy	0.72	0.88			
- RE1	0.88			0.01	119.83
- RE2	0.77			0.02	50.35
- RE3	0.88			0.01	106.24
Self-efficacy		1.00	1.00		
- SE2	1.00			NA	NA
Response costs		0.78	0.87		
- RC1	0.90			0.01	98.14
- RC2	0.87			0.01	68.15
Injunctive norms		0.78	0.91		
- IN1	0.89			0.01	79.20
- IN2	0.86			0.01	78.18
- IN3	0.90			0.01	92.89

Note. AVE: average variance extracted. CR: composite reliability.
[a]Bootstrap, N = 5,000.

Table 7.2 (continued): Coefficients of reliability and convergent validity

	Loading	AVE	CR	SE	t^a
Descriptive norms		0.76	0.90		
- DN1	0.87			0.01	68.24
- DN2	0.86			0.01	70.97
- DN3	0.88			0.01	85.58
Locus of control		0.64	0.84		
- LoC1	0.83			0.01	61.29
- LoC2	0.81			0.01	55.82
- LoC3	0.77			0.02	42.13
Protection motivation		0.80	0.94		
- PM1	0.88			0.01	70.66
- PM2	0.90			0.01	93.92
- PM3	0.90			0.01	125.07
- PM4	0.89			0.01	89.16

Note. AVE: average variance extracted. CR: composite reliability.
[a]Bootstrap, N = 5,000.

Table 7.3: Coefficients of discriminant validity

	PV	PS	PR	TR	RE	SE	RC	IN	DN	LoC	PM
PV	0.84										
PS	0.24	0.87									
PR	0.75	0.33	0.85								
TR	-0.37	-0.09	-0.45	0.85							
RE	-0.29	0.08	-0.32	0.46	0.85						
SE	-0.24	0.17	-0.24	0.26	0.57	1.00					
RC	0.26	-0.04	0.31	-0.20	-0.31	-0.40	0.88				
IN	0.20	0.03	0.21	0.00	0.02	-0.08	0.36	0.88			
DN	0.00	0.12	0.01	0.21	0.37	0.25	-0.03	0.19	0.87		
LoC	-0.29	0.08	-0.31	0.48	0.70	0.52	-0.29	0.03	0.34	0.80	
PM	-0.19	0.27	-0.16	0.28	0.71	0.65	-0.40	-0.04	0.36	0.61	0.89

Note. Off-diagonal values are correlations. Diagonal values are square root of average extracted variances. PV: perceived vulnerability. PS: perceived severity.PR: perceived risk. TR: trust. RE: response efficacy. SE: self-efficacy. RC: response costs. IN: injunctive norms. DN: descriptive norms. LoC: locus of control. PM: protection motivation.

Convergent validity – the extent of consistency among the items measuring a particular construct – was analysed using the average variance extracted (AVE) by a construct from its indicators, which should be 0.70 or higher (Henseler et al., 2009). All values exceeded this cut-off point with one exception: locus of control (AVE = 0.64); however, the AVE values exceeded 0.50, so – on average – more variability in the items of this scale was accounted for by its component than was not. Discriminant validity – the extent to which a measure of a particular construct differs from measures of other constructs – was assessed by analysing the square root of AVE by each construct from its indicators, which – according to the Fornell-Larcker-criterion – should be greater than its correlation with the remaining constructs. All values met this condition. Tolerance values

were well above 0.10 and VIF values were well below 10, indicating a lack of multicollinearity.[41] In conclusion, the reliability, and the convergent and discriminant validity of the multi-item constructs were confirmed. Per participant, a composite score was created for each of the factors, using the PLS weighted-average algorithm.

7.4.2 Structural Model

Descriptive statistics of the latent variables (Table 7.4) show that model variables with the highest mean scores (between 'agree' and 'strongly agree' on the response scale) were protection motivation, response efficacy and locus of control (the higher the score on locus of control the greater the internal control). Next-highest mean scores (between 'neither agree nor disagree' and 'agree' on the response scale) were for perceived severity, online-banking experience, trust, and descriptive norms. Variables with even lower mean scores (between 'disagree' and 'neither agree nor disagree') were perceived vulnerability, injunctive norms, perceived risk, and response costs.

Table 7.4: Descriptives and confidence intervals of model variables

	Mean	BCa 95% CI(mean)		*SD*
		Lower Limit	*Upper Limit*	
Perceived vulnerability	2.61	2.57	2.65	0.71
Perceived severity	3.96	3.92	4.00	0.76
Perceived risk	2.59	2.55	2.64	0.79
Trust	3.68	3.64	3.72	0.70
Response efficacy	4.18	4.14	4.22	0.67
Response costs	2.12	2.07	2.17	0.86
Injunctive norms	2.59	2.53	2.65	1.02
Descriptive norms	3.60	3.56	3.64	0.74
Locus of control	4.04	4.00	4.08	0.71
Protection motivation	4.38	4.35	4.42	0.64
Online-banking experience	3.83	3.77	3.89	1.09
Age	49.02	48.17	49.83	14.53

Note. BCa: bias-corrected and accelerated, N = 5,000.

The model variables and a selection of demographic variables were included in tests of the structural model. Demographic variables were selected if their correlation with protection motivation was at least .10 (small effect size for *r*; Cohen [1988]). Both online-banking experience and age met this condition and were therefore included. The results of testing the final structural model are presented in Table 7.5. Sixty-two per cent of variance in risk perception was explained by the predictors perceived vulnerability, perceived severity and trust. The strongest positive predictor was perceived vulnerability, followed by the

[41] Analysed with SPSS (version 23).

negative predictor trust, and the positive predictor perceived severity. Sixty-six per cent of variance in protection motivation was accounted for by the remaining variables. The strongest positive predictors were response efficacy and self-efficacy, followed by locus of control, perceived severity (direct effect) and the negative predictor response costs. A further significant predictor was risk perception, as were descriptive norms, trust (negative direct and indirect effect), perceived vulnerability (indirect effect), online-banking experience and perceived severity (indirect effect).

Table 7.5: Test results of the final structural model

Outcome variable	R^2	Predictor	Mediator	Beta	Standard error	t^a
Risk perception	0.62	Perceived vulnerability		0.63	0.02	29.64
		Perceived severity		0.16	0.02	8.00
		Trust		-0.21	0.02	8.86
Protection motivation	0.66	Risk perception		0.09	0.03	2.78
		Response efficacy		0.40	0.03	12.81
		Self-efficacy		0.26	0.03	9.03
		Response costs		-0.13	0.02	6.54
		Injunctive norms		-0.03	0.02	1.26
		Descriptive norms		0.08	0.02	4.15
		Locus of control		0.15	0.03	4.80
		Age		0.03	0.02	1.78
		Online-banking experience		0.05	0.02	2.91
		Perceived vulnerability		-0.03	0.03	1.25
		Perceived vulnerability	Risk perception	0.05	0.02	2.77
		Perceived severity		0.14	0.02	6.48
		Perceived severity	Risk perception	0.01	0.01	2.63
		Trust		-0.06	0.02	2.52
		Trust	Risk perception	-0.02	0.01	-2.60

[a]*Bootstrap, N = 5,000.*

Multi-group equivalence of structural model

Subgroups in a population may differ on the effect of predictors on outcomes. Any differences may have implications for security education, training and awareness campaigns, in which particular variables that are especially influential in a subgroup may be emphasized. Therefore, the equality of model parameters between different groups, defined by gender, age, and education level, was tested with Henseler et al.'s (2009) procedure.

Equivalence by gender. The results split by gender (Table 7.6) demonstrate significant differences between women and men on the predictors descriptive norms and age for the outcome variable protection motivation. First, the significant positive influence of the predictor descriptive norms was stronger in women than its non-significant positive influence in men. Therefore, women's protection motivation was more influenced by the extent they believe that other

people take precautions against security threats posed by online banking than is true for men. Second, the significant positive influence of the predictor age was stronger in women than its non-significant negative influence in men. Thus, with increasing age women's protection motivation increased, but this was not true for men.

Table 7.6: Analysis of model parameters by gender

Outcome variable	R^2		Predictor	Mediator	Female			Male			p(|female-male|)
	Female	Male			Beta	Standard error	t^a	Beta	Standard error	t^a	
Risk perception	0.59	0.65	PV		0.62	0.03	***20.78***	0.64	0.03	***20.93***	0.73
			PS		0.15	0.03	***5.44***	0.16	0.03	***4.64***	0.65
			TR		-0.22	0.03	***6.70***	-0.20	0.04	***1.98***	0.61
Protection motivation	0.68	0.66	PR		0.10	0.04	***2.65***	0.07	0.05	1.51	0.34
			RE		0.42	0.04	***10.67***	0.37	0.05	***7.32***	0.24
			SE		0.26	0.04	***7.03***	0.26	0.05	***5.54***	0.49
			RC		-0.15	0.03	***5.31***	-0.13	0.03	***3.85***	0.68
			IN		-0.01	0.02	0.48	-0.05	0.05	0.91	0.51
			DN		0.11	0.03	***4.26***	0.04	0.03	1.43	***0.05***
			LoC		0.11	0.04	***2.71***	0.21	0.05	***4.40***	0.94
			Age		0.07	0.02	***2.96***	-0.02	0.03	0.54	***0.01***
			OBX		0.03	0.02	1.16	0.07	0.03	***2.65***	0.91
			PV		-0.04	0.04	1.01	-0.04	0.04	0.82	0.53
			PV	PR	0.06	0.02	***2.61***	0.05	0.03	1.51	0.37
			PS		0.12	0.03	***4.60***	0.15	0.03	***4.64***	0.72
			PS	PR	0.01	0.01	***2.34***	0.01	0.01	1.49	0.39
			TR		-0.04	0.03	1.63	-0.08	0.04	***1.98***	0.22
			TR	PR	-0.02	0.01	***-2.45***	-0.02	0.01	-1.42	0.68

Note. PV: perceived vulnerability. PS: perceived severity. PR: perceived risk. TR: trust. RE: response efficacy. SE: self-efficacy. RC: response costs. IN: injunctive norms. DN: descriptive norms. LoC: locus of control. OBX: online-banking experience.
[a]Bootstrap, N = 5,000.

Equivalence by age. The results split by age (Table 7.7) show no significant differences between people age 50 or under and people aged over 50 on the predictors of risk perception or protection motivation. The age of 50 was used as the yardstick, as we wanted to test age groups of equal size but that also seem logical (672 ≤ 50 years, 528 > 50 years). Although differences between the groups were not significant, it is notable that the positive predictor risk perception in those over 50 was significant, but considerably smaller and not significant in those aged 50 or under.

Equivalence by education level. The results split by education level (Table 7.8) demonstrate significant differences between those with (N = 630) and without (N = 570) higher education on one predictor of risk perception – trust –, and two predictors of protection motivation – norms and trust (the latter with risk perception as mediator). First, the significant negative influence of the predictor trust on risk perception was stronger in those with higher education than its

Table 7.7: Analysis of model parameters by age

Outcome variable	R^2		Predictor	Mediator	Age ≤50			Age >50			p(|Age≤50->50|)
	Age ≤50	Age >50			Beta	Standard error	t^a	Beta	Standard error	t^a	
Risk perception	0.64	0.59	PV		0.64	0.03	***23.37***	0.62	0.03	***18.31***	0.37
			PS		0.16	0.03	***6.44***	0.16	0.04	***2.66***	0.49
			TR		-0.23	0.03	***7.83***	-0.18	0.04	0.06	0.83
Protection motivation	0.70	0.61	PR		0.04	0.04	1.15	0.13	0.05	***2.56***	0.91
			RE		0.39	0.04	***9.49***	0.42	0.05	***9.02***	0.68
			SE		0.29	0.04	***8.22***	0.21	0.05	***4.35***	0.10
			RC		-0.15	0.03	***5.82***	-0.11	0.03	***3.10***	0.83
			IN		-0.04	0.02	1.58	-0.03	0.04	0.72	0.73
			DN		0.08	0.03	***2.72***	0.09	0.03	***3.20***	0.62
			LoC		0.16	0.04	***3.91***	0.15	0.05	***3.20***	0.46
			OBX		0.06	0.02	***2.72***	0.05	0.03	1.77	0.34
			PV		0.00	0.04	0.07	-0.06	0.05	1.32	0.16
			PV	PR	0.03	0.02	1.14	0.08	0.03	***2.54***	0.90
			PS		0.16	0.03	***6.09***	0.10	0.04	***2.66***	0.07
			PS	PR	0.01	0.01	1.10	0.02	0.01	***2.36***	0.89
			TR		-0.11	0.03	***3.46***	0.00	0.04	0.06	0.98
			TR	PR	-0.01	0.01	-1.11	-0.02	0.01	***-2.11***	0.17

Note. PV: perceived vulnerability. PS: perceived severity. PR: perceived risk. TR: trust. RE: response efficacy. SE: self-efficacy. RC: response costs. IN: injunctive norms. DN: descriptive norms. LoC: locus of control. OBX: online-banking experience.
[a]Bootstrap, N = 5,000.

Table 7.8: Analysis of model parameters by education

Outcome variable	R^2		Predictor	Mediator	Higher education			No higher education			p(|HE-no HE|)
	HE	No HE			Beta	Standard error	t^a	Beta	Standard error	t^a	
Risk perception	0.62	0.62	PV		0.60	0.03	***19.67***	0.66	0.03	***21.73***	0.09
			PS		0.14	0.03	***5.21***	0.16	0.03	***5.57***	0.34
			TR		-0.25	0.03	***8.28***	-0.17	0.04	***4.66***	***0.04***
Protection motivation	0.64	0.70	PR		0.12	0.04	***2.88***	0.03	0.04	0.86	0.93
			RE		0.43	0.04	***10.97***	0.37	0.05	***7.32***	0.82
			SE		0.28	0.04	***6.91***	0.25	0.04	***5.90***	0.72
			RC		-0.12	0.03	***3.99***	-0.14	0.03	***4.94***	0.67
			IN		-0.03	0.05	0.67	-0.04	0.03	1.49	0.72
			DN		0.04	0.03	1.64	0.12	0.03	***4.02***	***0.02***
			LoC		0.13	0.04	***3.06***	0.16	0.05	***3.52***	0.27
			Age		0.03	0.03	1.12	0.03	0.02	1.05	0.60
			OBX		0.03	0.02	1.37	0.07	0.03	***2.60***	0.15
			PV		-0.07	0.04	1.69	0.01	0.03	***5.17***	0.08
			PV	PR	0.07	0.03	***2.86***	0.02	0.03	0.85	0.91
			PS		0.12	0.03	***4.13***	0.15	0.04	0.86	0.26
			PS	PR	0.02	0.01	***2.56***	0.01	0.01	0.83	0.89
			TR		-0.05	0.03	1.40	-0.07	0.04	1.89	0.66
			TR	PR	-0.03	0.01	***-2.63***	-0.01	0.01	-0.82	***0.04***

Note. PV: perceived vulnerability. PS: perceived severity. PR: perceived risk. TR: trust. RE: response efficacy. SE: self-efficacy. RC: response costs. IN: injunctive norms. DN: descriptive norms. LoC: locus of control. OBX: online-banking experience.
[a]Bootstrap, N = 5,000.

significant negative influence in those without higher education. Therefore, in those with higher education risk perception was more strongly negatively influenced by the extent to which they had trust in online banking than was true for those without higher education. Second, the significant positive influence of the predictor descriptive norms of protection motivation was stronger in those without higher education than its non-significant positive influence in those with higher education. Therefore, protection motivation of those without higher education was more influenced by the extent they believe that other people take precautions against security threats posed by online banking than was true for those with higher education. Third, the significant negative influence of the predictor trust, mediated by risk perception, on protection motivation was stronger in those with higher education than its non-significant negative influence in those without higher education. Therefore, in those with higher education protection motivation was more strongly negatively influenced by the extent to which they had trust in online banking (by reducing risk perception, which then decreased protection motivation), than was true for those without higher education.

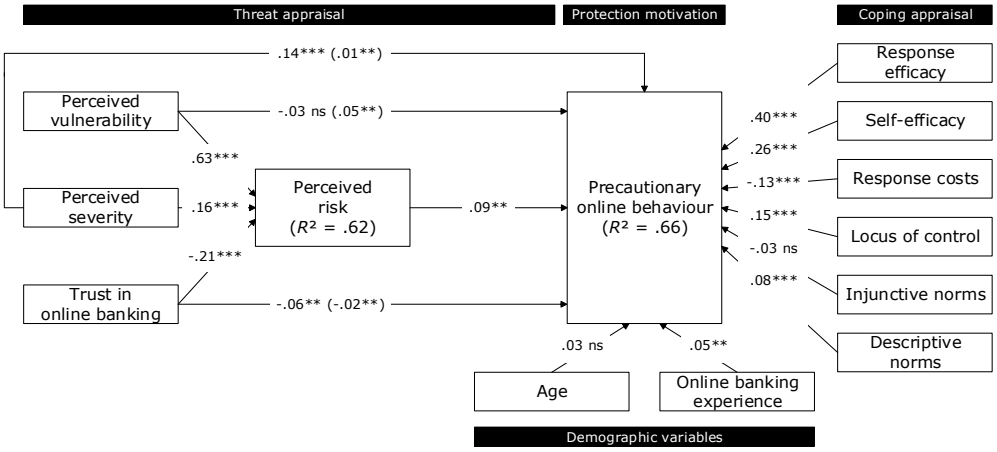
7.5 Conclusion and discussion

7.5.1 Exploration of main findings in relation to existing work

Overall, our model shows a large amount of explained variance for both risk perception and protection motivation. Explained variance of over 60 per cent is not exceptional in studies that have used PMT – or an extension of PMT – as their outcome variable (Ifinedo, 2012; Lee & Larsen, 2009). In Figure 7.2, the main findings are summarized. Except for H2b and H9, all hypotheses are supported, which indicates that the model has good explanatory power.

Considering risk perception, all measured predictor variables were significant and in the proposed direction, thus supporting H2a, H3a and H4a. This implies that when an online banking customer evaluates his chances to be defrauded as high – the most important predictor – and the potential impact of a fraud as high, he will perceive a higher level of risk. Conversely, if a customer has high levels of trust in online banking, then the level of risk perception is reduced. These findings are consistent with other studies on risk perception. Liang and Xue (2010), for example, found significant effects for the link from perceived vulnerability and perceived severity to perceived threat. Higher levels of trust leading to lower levels of risk perception is also found in earlier studies (Aldás-Manzano, Lassala-Navarré, Ruiz-Mafé, & Sanz-Blas, 2009; Grabner-Kräuter & Faullant, 2008; Yousafzai et al., 2009). The negative impact of trust on risk perception was strongest amongst highly educated respondents.

Figure 7.2: Summary of the results (final structural model)



*Note. ***p < .001, **p < .01, ns (not significant, i.e., p > .05), path-coefficients between brackets are mediated effects.*

Perceived threat has a positive influence on protection motivation, meaning that higher levels of perceived risk lead to the intention of precautionary online behaviour.[42] This is in accordance with literature (Liang & Xue, 2010), and leads us to support H1. However, the strength of perceived risk on protection motivation is modest. We interpret effect-sizes as proposed by Cohen (1988); small (.02), medium (.15) and large (.35). This outcome is consistent with the conclusions of a meta-analysis by Floyd et al. (2000), who mention that, in general, coping variables show a more strong and consistent relation with protection motivation than threat variables.

We also analysed effects of the predictors of perceived risk on protection motivation, both direct and mediated through perceived risk. Perceived vulnerability has a small, significant indirect effect and a non-significant direct effect on protection motivation, not supporting H2b. We found two studies who

[42] Unexpectedly, the correlation between perceived risk and protection motivation is negative, whereas the path-coefficient is positive. Liang and Xue (2010), who operationalized threat appraisal in a similar fashion, reported in their study a positive correlation and a positive path-coefficient. From studies that measured the effect of predictors of perceived threat – perceived vulnerability and perceived severity – directly on protection motivation and that included a correlation matrix, we observe both correlations and paths being positive (Ifinedo, 2012; Lee, 2011; Vance et al., 2012). Our result could be interpreted as effect reversal, a type of suppressive recast mediation (Koeske & Koeske, 2006). Based on additional analysis, it seems that response efficacy is responsible for the effect reversal.

also reported a non-significant direct linkage between perceived vulnerability and protection motivation (Gurung et al., 2009; Vance et al., 2012), whereby the first study reported that this outcome might be explained by a lack of knowledge of security measures by their respondents. However, other studies, such as those of Chenoweth et al. (2009), Lee (2011) and Workman et al. (2008), did find a positive direct linkage between these variables. Crossler (2010), who found a negative linkage between perceived vulnerability and backing up data, reasons that explanation of precautionary behaviour depends on the threats and behaviours studied and that future studies are needed to determine the true relationship of these constructs.

Perceived severity has a moderate, direct influence and a small, though significant, indirect influence on protection motivation, supporting H3b. Several studies who measured a direct linkage between perceived severity and protection motivation also found this relationship (Chenoweth et al., 2009; Gurung et al., 2009; Lee, 2011; Vance et al., 2012; Workman et al., 2008).

The significant negative (direct and moderated) effect of trust in online banking on protection motivation also seems logical, thereby supporting H4b. This means that when an individual puts a high level of trust in online banking, he or she is less inclined to take precautions.[43] This effect was again strongest amongst highly educated respondents.

The two most influential predictor variables for protection motivation are response efficacy and self-efficacy. Thus, the more effective a measure is perceived, and the higher one's confidence in his ability to take the measure, the more likely the intention to adopt this measure. These findings provide support of H5 and H6. These relations are supported by various studies (Crossler, 2010; Ifinedo, 2012; Johnston & Warkentin, 2010; Lai et al., 2012; Lee, 2011; Liang & Xue, 2010; Workman et al., 2008). The meta-analyses of Floyd et al. (2000) and Milne et al. (2000) also found these two variables to have the strongest predictive power for protection motivation.

[43] A similar unexpected change to the one before occurred between the variables trust and protection motivation, i.e., a positive correlation and a negative path-coefficient. Although this might indicate a multi-collinearity issue, we could not find any evidence for this from our results. Moreover, a unique feature of our model is the inclusion of the variable trust. In particular, we theoretically derived two hypotheses linking trust as a predictor to perceived risk and precautionary online behaviour as outcomes. However, our review of the literature showed no existing published peer-reviewed research that studied trust in relation to protection motivation. Therefore, future research is needed to find out whether trust can be considered a useful predictor of protection motivation.

Response costs have a negative relation with protection motivation, which in this case implies that when individuals consider the costs of a measure outweighs its benefits they are unlikely to perform precautionary online behaviour. This leads to the support of H7. This outcome is also supported by previous studies who have adopted PMT as a theoretical framework (Chenoweth et al., 2009; Lee, 2011; Liang & Xue, 2010; Vance et al., 2012).

The further coping variables also add explanatory power to the structural model, with (internal) locus of control amongst the strongest, supporting H8. When an individual believes that he is in control of the safety and security of online banking, he is more willingly to perform precautionary online behaviour. This is consistent with research of Ifinedo (2014) and Workman et al. (2008) who found a significant effect for locus of control on protection motivation. Customers must evaluate a threat as something that is within their control to prevent.

Considering social norms, only descriptive norms has a significant effect on protection motivation, implying that when individuals believe that others are taking precautions, they will actually do so as well. Herath and Rao (2009) found a similar effect. However, this relationship is only significant for the female population, not for the male population and for people without higher education as opposed to those with higher education. Injunctive norms were unsuccessful in explaining precautionary online behaviour. This contradicts with earlier studies (Herath & Rao, 2009; Ifinedo, 2012, 2014). However, the earlier studies measured norms within a business setting, whereas our study measured norms within a social setting. Our non-significant finding might be due to the behaviours studied or that safe online banking is not a topic frequently addressed in social conversations. Hence, apart from the small influence of descriptive norms, precautionary online behaviour related to online banking seems more an individual matter than a social issue. In sum, H10 is supported and H9 not.

Finally, two control variables are included in the final structural model. Although age was not a significant predictor variable for precautionary online behaviour, the influence of age differs between male and female respondents. With increasing age, women are more inclined to perform precautionary behaviour towards online banking than men, although the effect sizes are small in both conditions. The other control variable, online-banking experience, has a significant, though small, effect on protection motivation. This means that the longer a customer has made use of online banking services, the more inclined he is to have taken security measures. This finding may be related to Mannan and Van Oorschot's (2008) work; according to them, people who have adopted online banking later in life are less technically literate. Chen and Bansal (2010)

claim that previous experience can have an impact on individuals' security choices. This implies that more experienced online banking customers possibly better understand security issues and therefore are more motivated to behave cautiously.

7.5.2 Implications of the research model and future work

The first implication of our study is that the research model we proposed – which integrates additional variables within the PMT framework – is tested within the online banking context, making it a valuable tool for researchers studying protective behaviours in this context and for practitioners designing security education, training and awareness campaigns. Like others (Herath & Rao, 2009; Ifinedo, 2012), our study shows that it is fruitful to integrate theoretical perspectives from different domains. However, our work uniquely demonstrates this in the domain of online banking.

Second, from a practical point of view, this study broadens our knowledge regarding behavioural intention of customers to take precautions against online threats and what influences that behaviour. By these means, prevention programs can be enhanced. Current campaigns often focus on recommending to take basic measures, not considering underlying cognitive dimensions. An interesting approach in improving security education, training and awareness campaigns lies within the coping appraisal process. From our results, the most important variables to consider when designing education and training material and campaigns are response efficacy and self-efficacy. This implies that the efficacy of precautionary measures promoting safe online banking behaviour should be clearly communicated and that these measures are easy to apply, for example by presenting clear instructions or by showing how others – people with whom target groups can identify with – apply these measures. Furthermore, the costs of the precautions – both tangible and intangible – should be kept low. Hence, it is important for banks to find an optimal balance between the security and usability of their services. However, note that cross-sectional research cannot provide definitive answers about causality. Longitudinal or experimental research designs are required to explicitly define how the relationships between the dependent and independent variables work.

Locus of control is also considered an important variable predicting protection motivation. Therefore, banks should communicate that incidents related to online banking, such as phishing and malware victimization can be prevented, especially by efforts of customers themselves. When expectations are managed effectively, we expect customers to feel more in control about their online safety and, consequently, to take protective measures more easily. Moreover, stressing personal responsibility in communications to promote precautionary online

behaviour is supported by other research (Boehmer et al., 2015; Shillair et al., 2015).

Based on our results, security education, training and awareness campaigns could be more effective when the behaviours concerned are presented as the norm of what everyone does, especially for female customers and customers without higher education. Additionally, it might be beneficial to target efforts towards customers who have recently adopted online banking services, since online-banking experience also affects protection motivation but – by definition – new customers have limited experience.

Although the effect of the coping appraisal variables on protection motivation is large, attention should still be paid to threat appraisal variables, since they do provide explanatory power. Hence, when customers perceive risk to be low or are unaware of threats, they are less likely to behave precautionary online. Moreover, as proposed by PMT, the threat appraisal process is deemed essential for starting the coping appraisal process.

The outcomes regarding threat appraisal provide a paradoxical challenge for banks. For banks it is important that their target group is putting high levels of trust in their services since it reduces customers' security concerns. At the same time, banks have to educate customers about threats targeting online banking services, in order for them to take precautionary measures. Banks themselves have limited control over the safety and security of the online banking process. They can protect their own systems and can provide their customers a secure connection, but they have no control over customers' behaviour nor the (security of the) devices these customers use. We believe that customers should have or maintain a healthy dose of distrust or at least be adequately aware of the threats aimed at online banking, which also benefits banks. The challenge for banks is that they should inform and advise their customers in such a fashion that their customers become more resilient, but not evasive to using online banking services.

Regarding trust, we found that high levels of trust lead towards less protection motivation, especially for highly educated respondents. A plausible explanation for this finding might be that highly educated end users are confident in their own ability to get reimbursed by their bank when an incident does occur. Our reasoning follows a finding of Van Wilsem, Van der Meulen, and Kunst (2013), who found a linkage between education and successfully claiming losses from unjustified money transfers from banks. From this perspective, it seems that highly educated end users have reasons to trust online banking rather than worrying about risks.

The study also presents some limitations. We encountered problems with the self-efficacy scale. Although the scale itself was reliable, two of the three items loaded too heavily on protection motivation. Because of the demonstrated value of the self-efficacy construct in previous PMT-studies, we chose to include it, with only one item remaining, which limits its reliability. Moreover, single-item measures lead to lower predictive validity (Hair et al., 2014). Therefore, future research could benefit when including a more comprehensive set of items for this construct.

Another interesting issue is the relation between intention and actual behaviour. Our study focusses on intention. Although the linkage between intention and actual behaviour is evaluated as strong, consistent and theoretically grounded (Anderson & Agarwal, 2010), it is interesting to investigate this further, since there is often some discrepancy between what people report and what people do (Workman et al., 2008), that is the intention-behaviour gap. Sheeran (2002) argues, based on a meta-analysis of meta-analyses, that intentional behaviour on average explains future behaviour for 28 per cent. This may seem low, but the mean correlation Sheeran calculated between behavioural intention and actual behaviour is .53, which can be interpreted as a large effect size, indicating good explanatory power. Still, intentional behaviour and actual behaviour do not correlate perfectly. The intention-behaviour gap may be attributed to various causes such as the actual skills of people and environmental factors (Fishbein & Ajzen, 2010). Another factor that might influence behaviour – that is not mediated through intention – is habits or routines (O'Keefe, 2016).

Consequently, it might be informative to observe people's actual online precautionary behaviour, preferably over longer periods of time, for example by means of customer log-files in bank systems, diary research, eye-tracking studies or by analysing the software people have installed on their devices at their homes. Such efforts could furthermore rule out possible social desirability bias which is often found in survey studies. Obtaining actual behavioural data is, however, a challenge in behavioural information security research (Crossler et al., 2013). In addition, it might be relevant to study people's mental models about online banking threats and how those relate to precautionary measures (see e.g., Wash [2010]). This could be done by means of in-depth interviews and might increase our understanding on people's knowledge, intentions and actual behaviour and how these are related to each other.

Finally, the implications that are sketched in this section need to be tested in practice. This goes especially for the integrated variables outside PMT, because the beta coefficients regarding trust, social norms and demographics displayed

small effect sizes (i.e., well below .15). Although theory integration seems profitable, future research needs to test how meaningful the implications are when applied to practice. Having said that, Shillair et al. (2015) recommend experimental manipulations of PMT variables in order to convince individuals to protect themselves online. In agreement with this, Boss et al. (2015) recommend using fear appeals to enhance such behaviour. We believe that such studies are relevant in demonstrating the practical applicability of PMT. This could assist banks, for example, when launching new security applications.

7.5.3 Concluding remarks

The safety of online banking cannot be guaranteed solely by technical solutions, the human factor is important as well. If online banking customers do not take precautions, the safety of online banking may be easily compromised. This study developed and tested a model of precautionary online behaviour to explain why online banking customers take measures to protect themselves against online banking fraud. Our results show strong support for the model, not only for precautionary online behaviour but also for risk perception.

The most important conclusion of our study is that customers should have confidence in the efficacy of precautionary measures and in their own ability to actually perform a measure. These are the two most important factors leading to precautionary online behavioural intention. Moreover, both cognitive processes from PMT – threat and coping appraisal – are significant predictors of the intention to take precautionary measures. In sum, our study suggests that customer's precautionary online behaviour, ensuring a safer online-banking experience, can be enhanced by acknowledging these dimensions in security education, training and awareness campaigns.

The cognitive behavioural approach that we have taken in our study seems to be of added value of studying our research problem. It can help to improve the effectiveness of prevention efforts (Liang & Xue, 2010). We demonstrate that PMT – extended with additional, context-specific variables – can be a useful theory to apply to the online banking context, as proposed by Jansen (2015). Future (cross-cultural) research should further validate this model (Straub, 1989), both within and beyond the online banking context.

CHAPTER 8

Guarding against online threats: Why enterpreneurs take protective measures

Jurjen Jansen

Sander Veenstra

Renske Zuurveen

Wouter Stol

Published in Behaviour & Information Technology 2016, 35(5), 368–379.

8.1 Introduction

In today's society, the internet is becoming increasingly important for conducting business. Similar to the physical world, in the online world businesses need to deal with threats. In this study, we limited businesses to self-employed entrepreneurs, that is, own-account workers. Statistics Netherlands (CBS, 2014) reports that in Q2 of 2014, over 800,000 self-employed entrepreneurs were active in the Netherlands. This kind of entrepreneurship is on the rise, considering that the figure was 330,000 in 1996. Henceforth, we use the term entrepreneur to refer to self-employed entrepreneurs.

The internet has provided many opportunities for entrepreneurs. They use it for different purposes such as selling goods, gathering and storing data, communicating with clients and transferring money. The online sales volume in the Netherlands grew from 2.8 billion euros in 2003 to 10.6 billion euros in 2013 (www.thuiswinkel.org). At the same time, entrepreneurs are facing online threats as the internet attracts criminals. Entrepreneurs, like citizens, suffer from cybercrime. However, it is difficult to substantiate this claim with actual figures, since incidents are not likely to be reported to the police.

Cybercrime victim surveys in the Netherlands show that the percentage of crimes reported to the police is low for both citizens (13.4%; Domenie, Leukfeldt, Van Wilsem, Jansen, and Stol [2013]) and entrepreneurs (12.8%; Veenstra, Zuurveen, and Stol [2015]). Entrepreneurs may be reluctant to report incidents for several reasons, including the lack of financial damage, and perceptions that the incident is not serious enough or that the police are unable to solve the incident, and that the aftermath will result in reputation damage (Choo, 2011; Veenstra et al., 2015). These studies also point to the possibility that entrepreneurs may simply be unaware of the occurrence of online security incidents, and that incidents will be dealt with internally. Furthermore, cybercrime statistics in general are considered to be insufficient and fragmented (Anderson et al., 2012), and scientific research on cybercrime against businesses is scarce (Veenstra et al., 2015). Moreover, it is claimed that the current level of knowledge on crimes committed against micro, small and medium-sized businesses on the whole is limited (Schaper & Weber, 2012).

Veenstra et al. (2015) studied the extent to which entrepreneurs were victimised by 18 different forms of cybercrime, ranging from malware attacks to online extortion. They found that 28% of entrepreneurs in the Netherlands were victim of at least one type of cybercrime during the year prior to the study. From research into traditional forms of crime targeted against (all types of) Dutch businesses, it is known that 31% was victimised in the year prior to the study

(WODC & TNS NIPO, 2011). Although the target groups of both studies differ, the above implies that guarding against online risks, like offline risks, should be an important part of entrepreneurship. However, small businesses in general do not spend large amounts of time, effort or money on crime prevention strategies (Schaper & Weber, 2012). An earlier study among small and medium-sized enterprises in and around Amsterdam, for example, found that security expenses comprise around 1.0% of sales (Masurel, 2004). The same goes for cybercrime prevention strategies (Dimopoulos, Furnell, Jennex, & Kritharas, 2004; Gupta & Hammond, 2005; Sharma, Singh, & Sharma, 2009). It is also claimed that small businesses often have little or no IT security experience (Harris & Patten, 2014).

Since more and more business is taking place online, entrepreneurs quite often (28%) fall victim to cybercrime and entrepreneurs tend not to invest much in crime prevention strategies, it is essential to determine how entrepreneurs can be motivated to protect themselves against online threats. We are contributing to the literature by studying a target group that is often neglected in information security research, namely self-employed entrepreneurs. Currently, there is a lack of understanding on how and why entrepreneurs actually protect themselves against cybercrime. Based on secondary analyses of data from a large, representative sample of Dutch entrepreneurs (N = 1,622) (Veenstra et al., 2015), our aim is to gain insight into what protective measures entrepreneurs take in order to protect themselves against online threats and what motivates them to do so. We use protection motivation theory (PMT) as a theoretical lens to study the research problem. The justification for this approach is that a better understanding of motivations is a requirement to enhance awareness and prevention campaigns which address the problem of online threats (Lee, Larose, & Rifon, 2008). The remainder of this chapter is outlined as follows. We present PMT in Section 8.2, followed by our methodology in Section 8.3. We outline the results in Section 8.4, followed by a discussion and conclusions in Section 8.5.

8.2 Theory

PMT (Rogers, 1975) is a social cognitive model that predicts behaviour (Milne, Sheeran, & Orbell, 2000). With its basis in the health domain, PMT has recently been used to predict and explain the motivation for applying protective measures in information systems (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010; Vance, Siponen, & Pahnila, 2012) both in home and in business settings (Jansen, 2015).

The dependent variable in PMT research is protection motivation, that is, the intention to proceed, continue or avoid certain (protective) behaviour (Floyd,

Prentice-Dunn, & Rogers, 2000). In this study, PMT is applied to explain why entrepreneurs take protective measures to guard against online threats. The measures are divided into technical coping measures, such as installing anti-virus software, and personal coping measures, such as establishing rules for handling sensitive data. Instead of measuring 'intentional behaviour' as the dependent variable, as PMT suggests, we rely on 'self-reported actual behaviour' data gleaned from our dataset.

Two cognitive processes play an important part in explaining protection motivation, namely the threat appraisal process and the coping appraisal process. The first process constitutes an individual making an evaluation of the likelihood and severity of a threat. This process is performed initially, since a threat must be observed first before one can take actions against it (Floyd et al., 2000; Liang & Xue, 2009). The second process constitutes an individual making an evaluation of possible coping strategies.

8.2.1 Threat appraisal

PMT posits that when individuals perceive a threat, they will adjust their behaviour to the amount of risk they are willing to accept (Workman, Bommer, & Straub, 2008). As a result, we expect that perceived risk positively influences taking protective measures against cybercrime. Earlier studies on PMT have revealed this correlation (Lee & Larsen, 2009; Lee, 2011; Workman et al., 2008; Workman, Bommer, & Straub, 2009).

8.2.2 Coping appraisal

The predictor variables regarding coping appraisal are, according to PMT, response efficacy, self-efficacy and response costs. Response costs, however, are not operationalised in the study by Veenstra et al. (2015), and are therefore excluded from our study.

Response efficacy is the extent to which an individual believes a certain measure will be effective in reducing a threat (Milne et al., 2000). If an individual considers a measure to be effective, he or she will be more likely to implement it. We therefore reason that response efficacy positively influences taking protective measures. This relationship has been shown in several studies (Ifinedo, 2012; Lai, Li, & Hsieh, 2012; Lee & Larsen, 2009; Lee, 2011; Liang & Xue, 2010; Workman et al., 2008, 2009).

Self-efficacy 'concerns an individual's beliefs about whether he or she is able to perform the recommended coping response' (Milne et al., 2000, p. 109). The study by Veenstra et al. (2015) measured computer self-efficacy, which can be defined as 'an individual's perceptions of his or her ability to use computers in

the accomplishment of a task […]' (Compeau & Higgins, 1995, p. 191). For this study, we assume that computer self-efficacy is an indicator for self-efficacy in information security. Accordingly, if an individual possesses the required skills, he or she will be likely to implement protective measures. Thus, self-efficacy is expected to positively influence taking protective measures. This assumption is supported by previous studies (Ifinedo, 2012; Lai et al., 2012; Lee, 2011; Vance et al., 2012; Workman et al., 2008, 2009).

Based on the available data, we have added two additional variables to the coping appraisal process, namely attitude and locus of control, which may influence the outcome of the dependent variable. According to Fishbein and Ajzen (1975), attitudes are positive or negative feelings towards certain behaviour. In this study, it is hypothesised that a positive attitude towards measures positively influences taking protective measures. The relationship between attitude and behaviour is often revealed in information systems research (Venkatesh, Morris, Davis, & Davis, 2003).

Locus of control is the extent to which individuals believe certain outcomes are controlled by themselves (internal) or by others (external). Considering the safety and security of information (systems), people who perceive not being in control might assign responsibility to other parties, such as software developers, internet service providers or banks. External locus of control is undesirable since it is claimed that users themselves are vital for achieving online security (Davinson & Sillence, 2010; Liang & Xue, 2010). When people believe that safety and security are controlled by themselves and attribute responsibility to themselves accordingly, they are more likely to actively try to prevent online incidents from occurring (Workman et al., 2008). Consequently, we assume that internal locus of control influences the coping appraisal process by increasing the likelihood of taking protective measures. Studies by Workman et al. (2008, 2009) produced some evidence supporting this assumption. Research by Boehmer, LaRose, Rifon, Alhabash, and Cotten (2015) and Shillair et al. (2015), who both tested a concept similar to internal locus of control, namely personal responsibility, also found proof for this hypothesis.

8.2.3 Control variables

Finally, we include several control variables which might also be relevant in explaining the use of protective measures. The first one is 'experiences', which consists of one's internet experience (average time of use per day) and prior victimization. Chen and Bansal (2010), for example, argue that experienced internet users might have a better understanding of online security threats and, therefore, are more motivated to protect themselves. It is also claimed in the literature that individuals who are victimised once think they could easily be

victimised again (Workman et al., 2008), which might lead to greater motivation to protect oneself. The dataset provides us with information on prior victimization in phishing and malware attacks, two common schemes that are used to attack entrepreneurs' online banking services, for example. These are the most common attack types confronting entrepreneurs (Veenstra et al., 2015).

The second control variable is 'entrepreneur demographics', which consists of gender, age and educational level. These variables might be relevant in explaining which groups of entrepreneurs do a good – or not so good – job in protecting themselves against online threats.

The final control variables are two 'business characteristics': dependence on IT and the amount of confidential information stored. Our assumption is that entrepreneurs who perceive that their business is highly dependent on IT are more inclined to take protective measures related to information systems than entrepreneurs who are not dependent on IT. Similarly, entrepreneurs who store large amounts of confidential data in their systems, such as customer data, are more inclined to take protective measures than entrepreneurs who do not use their systems to store such confidential information.

8.3 Method

Prior research regarding online threats has focused on the general public or specific groups, such as youngsters. Knowledge regarding cybercrime is scarce among businesses. In 2014–2015, Veenstra et al. (2015) conducted a study on cybercrime victimization among entrepreneurs to augment the body of knowledge in this underdeveloped field of academic endeavour. Their study was commissioned by the Dutch National Police and its main goal was to gain insight into the nature and extent of cybercrime victimization. The methods used in the original study include a literature review, an online survey and interviews. We used only the data gathered in the online survey for our secondary analysis.

8.3.1 Data

Veenstra et al. (2015) used a questionnaire based on desk research, interviews with stakeholders, people from academia and cybercrime experts. The instrument was thoroughly pretested, both qualitatively (by scientific peers, an external advisory group of stakeholders, and entrepreneurs) and quantitatively, before the final version was put to use.

The Dutch Chamber of Commerce drew a sample of 10,277 entrepreneurs from their systems. They selected every 43rd entrepreneur from their alphabetically ordered database (N = 441,911). It is important to note that they could only

derive the addresses of entrepreneurs who had not opted out. Hence, not all Dutch entrepreneurs could be selected from this system. The researchers then entered the selected addresses in SPSS and randomly selected 10,000 addresses.

The selected entrepreneurs received a letter (followed by a reminder if they failed to respond) in which they were asked to participate in the study. The letter was sent in the name of the Dutch Police and included a unique log-in code giving entrepreneurs access to the online survey (which was available from 2 June to 1 July 2014, and hosted via a secure connection), and the possibility to complete it just once. In addition, an announcement of the study was put online on the website of the Dutch Police and on the websites of several special interest groups in order to convince entrepreneurs of the legitimacy of the study. Respondent characteristics are presented in Table 8.1.

Table 8.1: Descriptive statistics (N = 1,622)

Respondent characteristics	Count	Percentage
Gender		
Female	477	29.4
Male	1,145	70.6
Age		
< 25 years	18	1.1
25-35 years	166	10.2
36-45 years	352	21.7
46-55 years	510	31.4
56-65 years	403	24.8
> 65 years	173	10.7
Education		
Low (no, primary or lower secondary education[a])	276	17,0
Medium (upper secondary education[b])	514	31.7
High (higher education[c])	832	51.3

Note. [a]No education, primary education, lower vocational education and lower general secondary education. [b]Higher general secondary education, pre-university education and secondary vocational education. [c]Higher professional education and university education.

Ultimately, 9,893 entrepreneurs received the invitation letter; 107 were returned to the sender. Of the 2,088 entrepreneurs who started the questionnaire, 1,976 completely filled it in. Of these, 354 completed questionnaires were excluded afterwards, because these respondents did not belong to the intended target group, that is, entrepreneurs with employees, inactive entrepreneurs and entrepreneurs who do not use the internet. The results reported in this chapter are thus based on the answers provided by 1,622 entrepreneurs, a response rate of 16.4%.

8.3.2 Secondary analyses

The aim of this study is to gain insight into the extent to which entrepreneurs protect themselves against online threats and what motivates them to do so. Since the data are derived from a study that did not use PMT as a theoretical lens, the opportunities to operationalise the central concepts of the theory are limited. Appendix IV includes a description of how PMT variables were operationalised within the scope of the dataset. In addition, means and standard deviations are presented for each item. Self-efficacy was operationalised as a multi-item construct ($\alpha = .96$).

IBM SPSS Statistics version 21 was used to conduct the analyses. Because the dependent variables are dichotomous (i.e., taking all technical coping measures [yes/no] and taking all personal coping measures [yes/no]), we made use of logistic regression analyses. The predictive ability of all independent variables was assessed via the Forced Entry Method, while controlling for the effects of other independent variables in the model. We chose for a default procedure of logistic regression analyses because of the exploratory nature of our study. We disregarded other techniques such as stepwise procedures, because they can be biased by random variation in the data (Pallant, 2013).

Before running the analyses, the independent variables were checked for multicollinearity by means of standard multiple regression analyses. Correlations and collinearity diagnostics showed no signs of multicollinearity, meaning that the independent variables were not strongly correlated (see Appendix IV). Bivariate correlations between predictor variables and the dependent variable in both models did not exceed the cut-off point of .70. Collinearity diagnostics provided tolerance values well above .10 and VIF (variance inflation factor) values well below 10 (Pallant, 2013).

8.4 Results

This section presents results regarding protection against online threats. First, we discuss the protective measures entrepreneurs take against online threats (8.4.1). Second, we present the regression models and we outline the results regarding predictor variables (8.4.2).

8.4.1 Protective measures

The literature suggests that the adoption of protective measures to combat cybercrime is important. However, this poses a challenge particularly for small businesses due to a lack of resources (Gupta & Hammond 2005; Schaper & Weber 2012; Sharma et al., 2009). Entrepreneurs were, therefore, asked to what extent they take measures in order to cope with online risks. They

responded to four technical coping measures and four personal coping measures.

Almost all of the entrepreneurs have taken one or more technical coping measures. Most entrepreneurs use anti-virus software (92.7%), up-to-date software (91.2%), a secure network (91.0%) and a firewall (89.5%). Some 76.0% of the entrepreneurs have taken all four technical coping measures. Eleven entrepreneurs (0.7%) indicate not having taken any of the technical coping measures queried.

More than 90% of the entrepreneurs apply rules for opening potentially unreliable files (93.2%) and for providing data to third parties (91.9%). In addition, the majority of the entrepreneurs adopt rules for dealing with confidential information (82.6%) and making digital payments (81.8%). In all, 72.9% of the entrepreneurs take all four personal coping measures. In total, 63 entrepreneurs (5.0%) indicate not having taken any of the personal coping measures queried.

In summary, entrepreneurs take various measures to protect themselves against online threats.

8.4.2 Regression models

Direct logistic regression was performed to evaluate the impact of a number of factors on the likelihood that entrepreneurs will take protective measures. The first model explains 21.1% (Nagelkerke R^2) of the variance in taking technical coping measures (Table 8.2). The second model explains 19.3% (Nagelkerke R^2) of the variance in taking personal coping measures (Table 8.3).

As shown in Tables 8.2 and 8.3, all coping variables make a statistically significant contribution to the models (response efficacy, self-efficacy, attitude and locus of control). The demographic variables of age and education level are also significant predictors in both models. It can be concluded that prior victimization (Table 8.2) and having stored confidential information (Table 8.3) significantly contribute to explaining entrepreneurs' motivation for taking protective measures.

Regarding threat appraisal, 70.6% of the entrepreneurs indicate being worried about online risks to a (very) large extent. However, we did not find any evidence that worry begets action in the sense of taking technical and personal coping measures.

Table 8.2: Regression model for technical coping measures

	B	S.E.	Exp(B)
Constant***	-6.414	0.606	0.002
Threat appraisal			
Perceived risk	0.116	0.092	1.123
Coping appraisal			
Response efficacy***	0.673	0.105	1.961
Self-efficacy***	0.832	0.118	2.299
Attitude***	0.321	0.086	1.379
Locus of control***	0.307	0.081	1.360
Prior experience			
Internet	-0.087	0.064	0.917
Victimization**	0.568	0.186	1.765
Entrepreneur demographics			
Gender (ref. male)	0.132	0.139	1.141
Age**	0.157	0.058	1.170
Education (ref. high)***	-0.521	0.145	0.594
Business characteristics			
IT dependence	-0.081	0.053	0.922
Confidential information	0.033	0.050	1.034

*Note. ***p < .001, **p < .01*

Table 8.3: Regression model for personal coping measures

	B	S.E.	Exp(B)
Constant***	-5.917	0.577	0.856
Threat appraisal			
Perceived risk	0.037	0.087	1.037
Coping appraisal			
Response efficacy***	0.532	0.099	1.702
Self-efficacy***	0.748	0.113	2.113
Attitude***	0.395	0.083	1.484
Locus of control***	0.358	0.078	1.430
Prior experience			
Internet	-0.011	0.060	0.989
Victimization	-0.146	0.160	0.864
Entrepreneur demographics			
Gender (ref. male)	0.094	0.133	1.099
Age***	0.242	0.055	1.274
Education (ref. high)***	-0.497	0.138	0.608
Business characteristics			
IT dependence	-0.057	0.051	0.945
Confidential information**	-0.155	0.050	0.856

*Note. ***p < .001, **p < .01*

Regarding coping appraisal, it is clear that more than half of the entrepreneurs is (very) much confident in the efficacy of measures (53.7%); 4.0% has (very) little or no confidence. Both regression models show a positive significant relationship between having confidence in measures and taking measures.

Furthermore, entrepreneurs tend to report having the required skills to use computer and online technologies. The mean score was 3.0 on a 4-point Likert

scale. We observe from the regression models that self-efficacy is positively related to having taken both technical and personal coping measures. In fact, it is the strongest predictor variable in both models.

Regarding attitude, 67.6% of the entrepreneurs find information security (very) important for their business, while 5.6% thinks this information security is (very) unimportant. It can be observed in both models that a positive attitude has a significant relationship with the implementation of the protective measures queried.

In total, 89.7% of the entrepreneurs feel that they are responsible for keeping their information systems safe. Both regression models indicate the assumed relationship between internal locus of control and taking protective measures.

About one-third (34.8%) of the entrepreneurs use the internet on a limited basis, that is, less than 2 hours a day. This includes internet usage for both private and corporate purposes. In all, 10% of the entrepreneurs indicate using the internet over 8 hours a day. The regression analyses show no significant relationship between internet usage and taking protective measures.

Regarding prior experiences, we also asked whether entrepreneurs have been the victim of malware and phishing attacks. In total, 14.2% of the entrepreneurs indicated being victimised at least once by a malware attack, and 4.7% have been confronted with a successful phishing attack at least once. In order to filter out respondents who, for example, received a message from their anti-virus software that a malware threat had been successfully countered, or who simply received a phishing e-mail that they immediately deleted, Veenstra et al. (2015) explicitly differentiated between being victimised and having encountered an (unsuccessful) attempt. In total, 16.6% of entrepreneurs were considered a victim of a malware and/or phishing attack. Results show that prior victimization is a significant predictor for taking technical coping measures.

When taking into account the demographic characteristics of entrepreneurs, we notice two significant predictor variables in both regression models. The first predictor variable is age. Our analyses show that the older the entrepreneur, the more likely it is that he or she will have taken technical and personal coping measures. The second predictor variable is educational level (high vs. low and medium). We observe here, in both models, that the higher the entrepreneurs' level of education, the less inclined they are to take protective measures.

Finally, we observe two kinds of business characteristics, namely IT dependency and level of confidential information stored. Nearly two-thirds of the entrepreneurs report being fully or to a (very) large extent dependent on

information technology (63.3%). In 45.1% of the cases, entrepreneurs store confidential information on their computer systems to a (very) large extent. We found one significant relationship in this regard, namely a negative relationship between having stored confidential information and taking personal coping measures.

8.5 Conclusion and discussion

For entrepreneurs, it is important that their IT systems are secure and function properly, especially considering the fact that almost two-thirds of the entrepreneurs depend on IT to a very large extent. Keeping IT systems secure involves both technology and people (Huang, Rau, & Salvendy, 2010). We note that most entrepreneurs take one or more technical and personal coping measures in order to prevent online incidents. This leads to the conclusion that entrepreneurs in general do a decent job of protecting themselves against online threats. A limitation here is that only eight coping measures were studied. A study among IT practitioners in five different countries concludes that businesses across all company-sizes and industries do too little to prevent cybercrime (Ponemon Institute, 2012), especially when it comes to more advanced precautionary measures. It can be assumed that this also holds for entrepreneurs. Future research should include additional coping measures or more specific ones in order to paint a more complete picture of how entrepreneurs protect themselves against online threats.

A less optimistic picture emerges when we critically evaluate the response rate. Although a response rate of 16.4% is sufficiently large to make valid statements, entrepreneurs' interest in cybersecurity may not reliably be represented. It is quite possible that entrepreneurs were more likely to respond if they had a greater interest in this topic and/or if they had been victim of one or more forms of cybercrime at some point in the past. Those who did not respond may be less interested in cybersecurity and may not be likely to take adequate precautions against online threats. The main reason for not participating, based on a small non-response study (N = 26), however, was a lack of time – as time is money (Veenstra et al., 2015). Thus, this study cannot address the scope of inadequate online protection.

In addition, although the majority of entrepreneurs who responded to our study take measures against online threats, about a quarter still reports being victimised by cybercrime. This implies that there is still room for improvement and consequently that it is important to educate entrepreneurs and encourage them to take (additional and/or more effective) measures to protect their systems and data.

We found self-efficacy to be the strongest predictor variable for the application of protective measures. Self-efficacy has a strong impact on protection motivation, which is in line with various PMT studies (Floyd et al., 2000; Milne et al., 2000). Thus, having confidence in possessing adequate skills increases the odds of taking protective measures. This implies that education and/or training in this area could be of added value to entrepreneurs when it comes to safeguarding their business.

Another significant predictor for taking protective measures is response efficacy, meaning that increased confidence in the deterrent effect of measures increases the likelihood that the individual will take those measures. This means that entrepreneurs should be made aware of the efficacy of measures and learn more about how they work.

In line with the above, entrepreneurs should be made aware of the importance of measures, because having a positive attitude towards taking protective measures increases the likelihood that entrepreneurs will actually take them. In addition, it is advisable to communicate to entrepreneurs that they are in control of their own online security and that threats can be mitigated by means of their own efforts, hence emphasising their own responsibility. If an entrepreneur is confident that he or she is in control of the situation and feels responsible for his or her own online security (internal locus of control), the likelihood of taking measures increases.

The importance of encouraging personal responsibility has been demonstrated in recent studies (Boehmer et al., 2015; Shillair et al., 2015). Shillair et al. (2015) recommend, based on an experimental study among a representative sample of internet users, emphasising personal responsibility towards users with little knowledge about online protective measures in order to strengthen protection motivation. More experienced users benefit from an emphasis on shared responsibility. Thus, they stress the importance of using a segmented approach based on prior knowledge. Boehmer et al. (2015), who conducted a study among university students, mention that online safety messages addressing personal responsibility help motivate users to take precautionary measures, but could backfire when presented to users who are uninvolved in security issues and who demonstrate low levels of self-efficacy. The findings above may be important for the entrepreneur population as well, and they provide an interesting perspective for future research.

Generally speaking, educating entrepreneurs about the PMT coping appraisal process would seem to be called for. All measured variables in this cognitive process are significant predictors for taking protective measures. This means

that in prevention campaigns, information should be provided about the effectiveness of security measures and how to apply them, for example, by presenting clear instructions, providing information on why protecting systems and data are essential and emphasising the level of control entrepreneurs have in this regard.

We also found that entrepreneurs who had been victimised by a malware and/or a phishing attack were more likely to have adopted technical security measures. This finding could be used to perform digital penetration tests on entrepreneurs' computer systems or simulated social engineering attacks on entrepreneurs themselves. Once entrepreneurs are confronted with a security problem, they might feel the urge to protect themselves.

In addition, it might be relevant to study to what extent measures were adopted at the time entrepreneurs were victimised. Perhaps not all measures are effective in preventing incidents. Our study started with the assumption that there is a positive relationship between taking protective measures and maintaining online safety and security. In order to test this assumption, it would be beneficial to conduct effect studies of individual or combined protective measures. However, it will be difficult to determine the exact effects of these measures, because internet applications and online threats are constantly changing. Furthermore, the current data give no insight into the cause-and-effect sequence. Longitudinal research and in-depth analyses into this area might reveal important insights into revictimization as well.

Considering demographic variables, we noticed that older entrepreneurs take measures to protect their IT systems and data to a greater extent than their younger counterparts. Perhaps older entrepreneurs are more aware of their relative incompetence regarding online security and are, therefore, more likely to take measures to protect themselves. Additional analysis of variance showed that entrepreneurs in the older age categories (56–65 years, $M = 2.8$; >65 years, $M = 2.6$) reported having the lowest levels of self-efficacy compared to entrepreneurs in the younger age categories. Another possibility is that, perhaps because of their age, older entrepreneurs are simply more cautious than their younger colleagues. This corresponds to studies that show that younger adults are more careless regarding online security issues (Boehmer et al., 2015; Furnell, 2008b). We also found that the adoption of the measures queried decreases as the level of education increases. Perhaps highly educated entrepreneurs overestimate themselves, and are convinced that they will not fall victim to online scams or that their systems will not be compromised. Future research is needed to reveal if these claims are true.

Regarding business characteristics, we made a peculiar observation: the more confidential data an entrepreneur has stored on his or her system, the less likely he or she is to have adopted personal coping measures. We do not have a direct explanation for this outcome. Perhaps these entrepreneurs rely fully on their technical coping measures as opposed to their personal measures when it comes to securing such information. Another explanation might be that they feel beyond a doubt that confidential data should be treated diligently and that they, therefore, do not relate to this security need by taking personal measures. Accordingly, this issue is both interesting and concerning, and is worthy of further research.

Supplementary socio-demographic and business characteristics (e.g., prior knowledge, online security involvement, business sector and revenue) might be included in future studies in order to increase the predictive power of the models. Moreover, such characteristics could potentially be used to target particular prevention campaigns at specific groups of entrepreneurs as discussed earlier.

Over two-thirds of the entrepreneurs worry about their online security. However, perceived risk was not a predictor variable for taking protective measures. We believe that this might have to do with survey questioning. Only one item was included in the original study that could be translated into risk perception to some extent. Future research could perhaps find a relationship between perceived risk and taking measures when operationalised in a different, more reliable fashion, for example, by differentiating between perceived vulnerability and perceived severity. After all, PMT posits that the threat appraisal process initiates the coping appraisal process. Internet experience was also not a predictor variable for taking measures.

Overall, entrepreneurs generally tend to take measures against online threats as things stand. However, much still needs to be done to enhance their resilience to online threats. Raising awareness and training are therefore essential. Governmental agencies or professional associations for entrepreneurs may have a key role to play in this respect. Schaper and Weber (2012, p. 353) state in this regard: 'The most vigilant community is often the best-educated community'. PMT offers a useful starting point to enhance current prevention programs.

The present study makes an effort in this regard, although the design of the original study presents some limitations. Because the original study was exploratory in nature, focusing on a wide range of topics and was not developed with PMT in mind, most of the variables we tested, self-efficacy excluded, were operationalised as a single item. This limits the reliability of the results.

Therefore, the results should be interpreted with some caution, as they merely present an exploratory observation on the problem. Although self-efficacy was included as a scale variable, it measured competence in the use of computers and online technologies (Sam, Othman, & Nordin, 2005; Torkzadeh & Koufteros, 1994), rather than skills related to applying security measures, which could have increased its predictive value (Rhee, Kim, & Ryu, 2009). Likewise, locus of control is reflected by a single item explicitly relating to responsibility, neglecting items regarding the entrepreneurs' level of control for outcomes.

Future research should include validated PMT scales (e.g., Witte, 1996) for a more reliable investigation of the problem. Response costs should be included as well, because these are considered to be an important predictor variable in PMT and an important factor in business strategies. If a measure's costs are higher than an entrepreneur's perception of the measure's effects, protection motivation may suffer.

In conclusion, the importance of online safety and security for entrepreneurs cannot be understated and in fact merits greater emphasis. Our study indicates that PMT provides a valuable approach in studying precautionary online behaviour and helping to improve entrepreneurs' security practices. More empirical studies should be carried out in order for PMT to achieve its full explanatory and/or predictive potential in this context.

CHAPTER 9

The design and evaluation of a theory-based intervention to promote security behaviour against phishing

Jurjen Jansen

Paul van Schaik

Submitted.

9.1 Introduction

End-users' information security practices play an essential role in mitigating threats such as phishing scams, malicious software and distributed denial-of-service attacks within modern, networked society. As more services are offered online and personal data are increasingly stored by digital means, people become more technology-dependent, but also more susceptible to security incidents (Furnell, Bryant, & Phippen, 2007). It is recognized that precautionary online behaviour by end users is important in safeguarding the online domain, because they play a central role in achieving online security (Furnell, Jusoh, & Katsabas, 2006; Liang & Xue, 2010; Ng, Kankanhalli, & Xu, 2009). This study investigates to what extent fear appeals can persuade end users to perform safe online behaviour. Attention to fear and fear appeals is currently lacking in the information security domain (Johnston, Warkentin, & Siponen, 2015), but is gaining in popularity (Wall & Buche, 2017). Moreover, as stated by Briggs, Jeske, and Coventry (2016), the work on behaviour change interventions for cybersecurity is just getting started.

Michie, Van Stralen, and West (2011, p. 2) define behaviour change interventions as 'coordinated sets of activities designed to change specified behaviour patterns'. Interventions aimed at behavioural change are quite common in human-computer interaction studies, but less common in the field of information security (Coventry, Briggs, Jeske, & Van Moorsel, 2014). Persuading end users to adequately cope with cyber-threats will, however, not be an easy task. As noted by Fransen, Smit, and Verlegh (2015), persuasion plays a prominent role in everyday life, but persuasion efforts in themselves often have limited impact. They state that perhaps the most important reason for this is that individuals do not want to be influenced. Another potential reason is that people normally strive to reduce (mental) effort by relying on fast information-processing ('System 1') rather than on deliberate processing ('System 2') (Kahneman, 2011).

The current study focusses on protection against a specific online threat, namely phishing attacks, the process of retrieving personal information using deception through impersonation (Lastdrager, 2014). Phishing is considered dangerous to end users (Arachchilage, Love, & Beznosov, 2016; Arachchilage & Love, 2014; Hong, 2012; Kirlappos & Sasse, 2012) and forms a world-wide problem (APWG, 2015) for different sectors, such as the retail industry and banking organizations. For online banking for instance, it seems that everyone is susceptible to phishing to some degree (Jansen & Leukfeldt, 2015). However, it is argued that, 'an educated, informed and alert customer could play an

important role in improving online banking security and be better prepared against phishing attacks' (Purkait, 2012, p. 406).

Roughly four different types of intervention can be distinguished in promoting precautionary online behaviour by end users: security education, training, awareness-raising and design (Kirlappos & Sasse, 2012; Posey, Roberts, & Lowry, 2015; Van Schaik et al., 2017). Education involves developing knowledge and understanding of online threats and ways to mitigate threats, while training typically involves developing skills in information security. The aim of increased knowledge and skills is that they transfer to adequate levels of precautionary online behaviour (Van Schaik et al., 2017). Awareness-raising is involved with agenda-setting – or warning users – and focusses attention on threats and countermeasures. Effective security design should facilitate desirable user behaviour (Sasse, Brostoff, & Weirich, 2001). Design might involve nudges in the environment that gently push an end user, without too much mental effort, to perform the right behaviour (Coventry et al., 2014; French, 2011; Thaler & Sunstein, 2009), for instance by manipulating a default setting to protect user data (Briggs et al., 2016).

Technical and legal solutions to combat phishing have been proposed as well (Purkait, 2012). Examples of technical solutions include automated phishing tools, e-mail filters and blacklists (Arachchilage & Love, 2014; Hong, 2012; Ludl, McAllister, Kirda, & Kruegel, 2007), but these solutions provide certain drawbacks, such as false positives, false negatives and usability issues. In addition, safety cues tend to be ignored by end users (Dhamija, Tygar, & Hearst, 2006) and are also quite easy to manipulate by hackers (Downs, Holbrook, & Cranor, 2006). An eye-tracking experiment by Alsharnouby, Alaca, and Chiasson (2015) showed that their participants spend only 6% of the time looking at security indicators and 85% at the content of the webpage when deciding whether a website is legitimate or not. Other research also demonstrated that end users are more focussed on looking for signs that demonstrate trustworthiness than signs that prove security (Kirlappos & Sasse, 2012). In conclusion, technology alone cannot provide the complete security solution; human aspects are essential to address (Furnell & Clarke, 2012).

Although interventions are deemed important, the effectiveness of interventions is yet to be determined. In this study, we will focus on a combination of security education and awareness-raising, an approach which finds support from current literature on phishing (Arachchilage & Love, 2014; Downs, Holbrook, & Cranor, 2007; Purkait, 2012; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). Educating end users and implementation – and proper application – of precautionary online behaviour are critical in protecting against phishing attacks

(Butler, 2007; Purkait, 2012). Although education has its limitations, given the complexity of the problem and a lack of interest by non-specialist internet users (Jakobsson, 2007), and will not solve the phishing problem on its own (Alsharnouby et al., 2015), aware and vigilant end users who practice precautionary online behaviour are believed to better identify phishing attempts (Purkait, Kumar De, & Suar, 2014).

In this study, we focus on one type of behavioural context, that is sharing or disclosing personal information online. Personal information includes personally identifying, financial and demographic information (Norberg, Horne, & Horne, 2007). Putting personal information online makes it easy for criminals to take advantage of that information (Shillair et al., 2015). Sharing personal information, like e-mail address, telephone number, employer, insurance details, birthday, social security number, name and address, (publicly) online might provide fraudsters with opportunities to (spear) phish someone. An experimental study in an organizational setting by Rocha Flores, Holm, Svensson, and Ericsson (2014) showed that when more target information was added to an attack the likelihood of an organization employee falling for that attack increased. In addition, studies on phishing have demonstrated that an essential part in a fraudulent scheme to be effective is end users give away their personal information, for example user credentials (Hong, 2012; Jansen & Leukfeldt, 2015; Purkait, 2012). Therefore, demonstrating vigilant behaviour towards personal information sharing online is important to (a) prevent being attacked by means of phishing and (b) to prevent phishing attacks from succeeding.

The goal of our study is to gain insight into the effects of fear appeal manipulations on end-users' cognitions and subsequently on danger control (attitude, intentions and behaviour) and on fear control (resistance and avoidance). A novel contribution of this work is a focus on both danger control and fear control, which is ignored in most information security studies that focus solely on danger control (Boss, Galletta, Lowry, Moody, & Polak, 2015; Wall & Buche, 2017). Additionally, testing the effects of fear appeals in three experimental conditions is rare in information security studies. Furthermore, most studies within the information security domain focus on behavioural intention only which is considered a drawback (Boss et al., 2015; Crossler et al., 2013). Therefore, we investigate both behaviour and behavioural intention. Moreover, we examine the effects of fear appeals at two points in time, while most studies examine these at just one point in time (Wall & Buche, 2017). Finally, this study benefits from a large, non-student research sample.

9.2 Theory

9.2.1 Protection motivation theory

The leading theoretical framework used for this study is protection motivation theory (Maddux & Rogers, 1983; Rogers, 1975), henceforth PMT, originally developed to study disease prevention and health promotion (Floyd, Prentice-Dunn, & Rogers, 2000). Although the original purpose of PMT is to clarify fear appeals, it has been used as a more general model to study decisions related to risk (Maddux & Rogers, 1983). Recently, PMT has been applied to the information security domain (e.g., Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015; Boss et al., 2015; Jansen & Van Schaik, 2017; Johnston et al., 2015) providing opportunities to study end-users' motivation to perform precautionary online behaviour, a major focus in current (behavioural) information security literature (Boss et al., 2015).

9.2.2 Threat appraisal

Protection motivation is initiated by two appraisal processes. The first one is called threat appraisal, a process in which a person evaluates threats triggered by a fear appeal. More specifically, the person evaluates the vulnerability or probability of a threat occurring to him- or herself and the severity or impact of a threat.

PMT studies that examine motivations of end users performing precautionary online behaviour have found mixed results for the threat appraisal process. Some studies found both threat appraisal variables to be significant positive predictors (e.g., Chenoweth, Minch, & Gattiker, 2009; Lee & Larsen, 2009; Lee, 2011; Liang & Xue, 2010; Workman, Bommer, & Straub, 2009). However, one study found both threat appraisal variables to be significant, but negative predictors (Crossler, 2010) and in another study perceived vulnerability had a positive influence whereas perceived severity had a negative influence (Ifinedo, 2012). In other cases, only one of two threat appraisal variables were found to be significant predictors (e.g., Gurung, Luo, & Liao, 2009; Herath & Rao, 2009; Jansen & Van Schaik, 2017; Vance, Siponen, & Pahnila, 2012; Yoon, Hwang, & Kim, 2012).

Considering that the above mentioned studies focused on different kinds of protective behaviour within different contexts, it seems that the predictive ability of precautionary behaviour by threat appraisal depends on the threats and behaviours studied (see also Crossler [2010]). Johnston et al. (2015) attribute conflicting outcomes of PMT-variables to the misuse or misspecification of PMT in an information security context, for example by not paying adequate attention to the requirement that fear appeals must be personally relevant to a receiver,

or the fact that fear appeals were entirely missing from a study's operationalization.

Personal relevance or issue involvement is deemed essential in communications about information security (Johnston et al., 2015). This factor is especially important since the involvement of the audience in a certain topic determines to what extent one will focus on, elaborate on and comprehend a message (Petty & Cacioppo, 1986), thus potentially influencing the effect of a fear appeal (Johnston et al., 2015). Besides issue involvement, other factors that have an effect on the investment of cognitive resources include time pressure, skill level and distractions (Luo, Zhang, Burd, & Seazzu, 2012).

9.2.3 Coping appraisal

The second appraisal process is called coping appraisal, a process in which a person evaluates components of a fear appeal that relate to possible strategies to prevent threats or to minimize their impact. More specifically, it deals with the person's evaluation of the perceived effectiveness of the recommended response (response efficacy), the perceived ability or skills of oneself to perform the recommended response (self-efficacy) and the perceived barriers in performing the recommended response (response costs), for instance time and expenses (Milne, Sheeran, & Orbell, 2000).

Previous work on determinants of precautionary online behaviour shows that response efficacy and self-efficacy are the most influential predictor variables (Boehmer et al., 2015; Crossler, 2010; Ifinedo, 2012; Jansen & Van Schaik, 2017; Lee, 2011; Liang & Xue, 2010; Workman, Bommer, & Straub, 2008). This is also true for studies in the health domain. Indeed, the meta-analyses of Floyd et al. (2000) and Milne et al. (2000) of empirical PMT research and the meta-analysis of Witte and Allen (2000) of empirical research on fear appeals indicate that, in general, the coping variables show stronger relations with adaptive behaviours than the threat variables do.

Response costs have been found to be a significant (negative) predictor of precautionary online behaviour (Chenoweth et al., 2009; Herath & Rao, 2009; Jansen & Van Schaik, 2017; Lee, 2011; Liang & Xue, 2010; Vance et al., 2012) and may play an important part in making security-convenience trade-offs. Herley (2009) argues that end users make an implicit calculation of costs versus benefits when deciding to follow a certain piece of advice. He claims, however, that security advice often suffers from a poor trade-off and will therefore be neglected by end users.

9.2.4 Interventions based on protection motivation theory

When PMT is used as a theoretical basis for interventions, the focus is on the operation of fear appeals, which are 'informative communication[s] about a threat to an individual's well-being' (Milne et al., 2000, p. 107). Such communications also contain information on and promote perceptions of efficacy. Therefore, it would seem meaningful to speak of 'threat and efficacy appeals'. However, we will use the term 'fear appeals', as this is consistent with the literature. Fear appeals thus include elements to raise perceived threat and increase perceived efficacy of a recommended response. The latter seems an important requirement for fear appeals because threat messages in themselves, under low efficacy conditions, have almost no or even negative effects on behaviour (Kok, Bartholomew, Parcel, Gottlieb, & Fernández, 2014; Peters, Ruiter, & Kok, 2014). Witte and Allen (2000) also stress that fear appeals will only work when complemented by an equally strong efficacy message.

9.2.5 Protection motivation theory in relation to other theories

Other theories of fear-arousing communications include the parallel process model (Leventhal, 1970), the extended parallel process model (Witte, 1992), henceforth EPPM, and the stage model of processing of fear-arousing communications (Das, De Wit, & Stroebe, 2003; De Hoog, Stroebe, & De Wit, 2005). A difference between these theories and PMT is that the latter focusses on *danger control* responses only, that is an individual performing actions to mitigate a threat. In contrast, the other theories mentioned also focus on *fear control* responses, that is actions that do not affect the danger, such as avoidance and emotional coping strategies (De Hoog et al., 2005). In addition, the EPPM also focusses on *non-responses* and the stage model also considers modes and motives of information processing and additional outcome measures, namely attitudes, behavioural intention and behaviour.

Although PMT is the leading framework in the current study, we apply two additional components of the other theories to provide a more comprehensive view on the effects of the fear appeals studied. The first addition is that we study attitudes – both as an outcome variable and as a predictor of behavioural intention (Fishbein & Ajzen, 2010). This addition is consistent with the EPMM and with previous cybersecurity research using PMT (Jansen & Van Schaik, 2017). The second addition is that we study fear control. According to Witte and Allen (2000), fear appeals often target two types of outcome. Outcomes of the first type are related to message acceptance (danger control), measured in terms of attitude, intentions and behaviours. However, fear appeals might have a counterproductive effect in terms of outcomes of the second type, message rejection (fear control), such as avoidance, reactance and denial. Boss et al.

(2015) stress that it is important to study such possible effects as well. We adopt two types of message rejection: avoidance or risk denial (i.e., efforts to direct attention away from stress [Green, Choi, & Kane, 2010]) and resistance (i.e., reservations towards the behaviour that is aimed to be changed [Van Offenbeek, Boonstra, & Seo, 2013]). It could be that the results of acceptance and resistance contradict each other. We adopt the viewpoint of Van Offenbeek et al. (2013) who conceptualize acceptance and resistance as two separate dimensions rather than an opposite ends of a continuum. By studying both outcome types, our study provides a unique contribution to behavioural information security research.

9.2.6 Fear appeal manipulation

A meta-analysis on fear appeals by Witte and Allen (2000) shows that medium to strong effects were achieved by fear manipulations on perceived vulnerability, perceived severity, response efficacy and self-efficacy. When predictor variables of PMT were manipulated, small significant effects were found for attitudes, behavioural intentions and behaviours. However, the effects on subsequent behaviour are often limited (Floyd et al., 2000; Milne et al., 2000). For the information security context, studies have demonstrated that fear appeals are effective in promoting precautionary motivations and behaviours (Wall & Buche, 2017).

It is not precisely known which components or types of information in a fear appeal are effective (De Hoog et al., 2005; De Hoog, Stroebe, & de Wit, 2007), although response efficacy and self-efficacy seem more important than raising levels of risk and fear (Ruiter, Kessels, Peters, & Kok, 2014). It is also not yet clear how fear appeals specifically impact end-user behaviour within the information security context (Johnston et al., 2015; Johnston & Warkentin, 2010). However, a meta-analysis by Sheeran, Harris, and Epton (2014) regarding experimental studies on risk appraisals demonstrates that the largest effect sizes were observed for behavioural intention and behaviour when threat appraisal and coping appraisal variables were simultaneously heightened.

9.2.7 Research questions

The current study addresses the following research questions.[44]

[44] In this chapter, precautionary online behaviour and precautionary online behavioural intentions refer to demonstrating vigilance towards online information-sharing. Note that the latter is used synonymously with protection motivation.

RQ1: To what extent do end users share their personal information online?

RQ2: What effect do fear appeals have on end-users' cognitions (perceived vulnerability, perceived severity, fear, response efficacy, self-efficacy and response costs)?

RQ3: What effect do fear appeals have on end-users' attitudes towards precautionary online behaviour?

RQ4: What effect do fear appeals have on end-users' precautionary online behavioural intentions?

RQ5: To what extent is the effect of fear appeals, if any, stable over time?

RQ6: What effect do fear appeals have on end-users' precautionary online behaviour?

9.3 Method

9.3.1 Design

According to Milne et al. (2000) fear appeal intervention studies often comprise between a strong and a weak manipulation. This is because manipulations of argument strength are expected to have an effective impact on message processing (Petty & Cacioppo, 1986).[45] Furthermore, it is argued that argument quality – when processed via the central route – has a positive influence on attitudes (Bhattacherjee & Sanford, 2006; Meijnders, Midden, & Wilke, 2001). In contrast, Johnston et al. (2015) argue that in information security studies, there is a strong tradition of presenting one (or more than one) treatment to one group and no treatment to a control condition. Our study combined these viewpoints. Therefore we included the following three conditions: a strong intervention (strong fear appeal), a weak intervention (weak fear appeal) and no intervention (control condition). We chose to use an independent-measures design (one group for each condition) because this potentially increases external validity. In addition, it only requires one set of data per participant, making data collection convenient. The possible downside is that individual differences occur

[45] The elaboration likelihood model of persuasion (Petty & Cacioppo, 1986) assumes that attitudes are formed by a dual route. When individuals are involved with a certain topic the central route is followed (systematic processing). In that case, individuals actively process a message, because they are motivated and mentally capable of doing so. This might lead to long-term changes in attitudes and, consequently, possibly in behavioural change as well. When individuals lack the aforementioned characteristics, a peripheral route of information-processing is followed, which requires less effort (automated processing). The peripheral route will only lead to temporary attitude change. The content of a message, strong argumentation for example, is not relevant in this case, but the way in which it is presented to an individual, such as attractiveness of the message and reputation of the sender. Thus, the route being followed, or the means in which a message is processed, determines the response.

between the groups, potentially threatening the internal validity. However, this was limited by using a large sample and a stratified sampling method (controlling for gender and age).

We chose to collect data across two different periods of time. This is because the outcomes of an intervention should be stable over time (Milne, Orbell, & Sheeran, 2002). In order to establish this, a decision had to be made about the time between the two measurements. Davinson and Sillence (2010), for example, used a one-week interval for an experimental study on phishing, resulting in positive changes in both intentions and behaviour. Bullée, Montoya Morales, Junger, and Hartel (2016) demonstrated that the effects of an information campaign on social engineering attacks dissipated already after two weeks. However, a fear-appeal study by Milne et al. (2002) showed that the effects of a PMT-intervention lasted over two weeks. A study on phishing training by Kumaraguru et al. (2009) showed that knowledge retention lasted at least for 28 days. We argue that a timeframe of four weeks is reasonable and also necessary for participants in order to not remember exactly the answers they gave on the first measurement. Furthermore, we believe that a more frequent presentation of a fear appeal message, for example every two weeks, might cause end users information overload. Moreover, by using a four-week period, participants were more likely to encounter situations in which they had to make decisions related to personal information-sharing online.

At the first measurement (Time 1 [T1]), participants received a strong fear appeal message, a weak fear appeal message or no message, and they all filled out the same questionnaire immediately afterwards. This gave us the opportunity to analyse whether user-perceptions were elevated by means of the (strength of the) fear appeal. We decided not to use a baseline measurement, since it was expected that the study participants already had some beliefs on phishing and on the recommended response. As noted by Johnston and Warkentin (2010), fear appeals may reinforce or elevate these beliefs, but in any case users will take action if adequately motivated. The purpose of our study was to investigate the strength of this reaction, justifying our decision to not include a baseline survey. In any case, our control condition provided a baseline comparison with the two experimental groups.

At the second measurement (Time 2 [T2]), participants received a similar questionnaire, including all PMT-related items from the previous questionnaire and their information-sharing behaviour in the past month. This was done to study whether possible effect of the fear appeal would last over time and whether intentions were acted upon.

Fear-appeal design

A meta-analysis of empirical fear appeals research by De Hoog et al. (2007) showed no significant differences between fear appeals that used vivid images and fear appeals that used written information only. Therefore, our study involved the manipulation of a written communication, targeting particular PMT-variables. Following the advice of Kirlappos and Sasse (2012), we focused on equipping 'users to assess the potential risks and benefits correctly', rather than telling them to completely avoid certain kind of behaviour. In addition, we followed their advice in making the fear appeal threat-specific.

The fear appeals were presented by means of a self-developed text, which participants were required to read. The text contained factual information on phishing (victimization) and the effects of sharing personal information online – based on results from Bursztein et al. (2014) and Kloosterman (2015) – and was presented digitally to the participants – within the survey environment. We followed a similar approach like that of De Hoog et al. (2005), by designing a fear appeal with strong arguments and a fear appeal with weak arguments. The PMT-variables perceived vulnerability, perceived severity, response efficacy and self-efficacy were targeted in the fear appeals, as the combined manipulation of threat appraisal and coping appraisal variables showed the largest effect on the outcomes (Sheeran et al., 2014). We also followed a recommendation of Ruiter et al. (2014) by making no emotional statements about threat severity.

Because PMT posits that threat appraisal occurs first (Floyd et al., 2000), the fear appeal messages started by highlighting information regarding phishing vulnerability and severity. We tried to evoke personal relevance by means of perceived vulnerability, addressing the potential of being personally victimized. The emphasis of perceived vulnerability in the strong fear appeal was on the extreme, being almost unable to escape from phishing attacks, whereas the weak fear appeal nuanced the chance of victimization by a phishing attack.

According to PMT, coping appraisal takes place after a threat has been evaluated. Thus, the fear appeal messages continued with information on response efficacy and self-efficacy. Therefore, arguments needed to be constructed that promote the effectiveness and usability of the measure. We primarily focussed on arguments regarding response efficacy, because this variable showed strongest predictive ability in previous research. The emphasis of response efficacy in the strong fear appeal was framed as being very effective, that is not sharing personal information online will lead to not being attacked by phishing and any phishing attack that may happen not being successful. In contrast, in the weak fear appeal the level of efficacy was downgraded.

After the fear appeals were constructed, they were critically reviewed by four of our colleagues who are experts in online safety and security. Brown and Whiting (2014) argue that self-assessment or a review by colleagues is an adequate means for ethical review when fear appeals comprise the mere release of information to a general population. The expert review led to three main changes: (1) a more active phrasing of sentences, (2) balancing the number of arguments in both fear appeals, and (3) shortening the length of the fear appeals. The fear appeal messages can be found in Appendix V.

Survey questionnaire and procedure

A questionnaire was developed based on a review of the literature, using the following international databases: ACM Digital Library, ScienceDirect and Web of Science. We included items that represent PMT's core predictor variables: perceived vulnerability, perceived severity, response efficacy, self-efficacy and response costs. The outcome variables were attitude towards behaviour, fear, behavioural intention, online information-sharing behaviour and message rejection (i.e., resistance and avoidance). Attitude and fear were also identified as predictors of intentions.

The questionnaire items were based on the work of Anderson and Agarwal (2010), Brouwers and Sorrentino (1993), Davis (1993), Ifinedo (2012), Johnston et al. (2015), Milne et al. (2002), Ng et al. (2009), Witte (1994; 1996), and Witte, Berkowitz, Cameron, and McKeon (1998). The items used a 5-point Likert scale (totally disagree – totally agree), with the exception of attitude which used a 5-point semantic differential scale, were translated in Dutch and were presented in random order. The questionnaire items and the sources we based them on can be found in Appendix V. In order to counter possible memory effects, the order of the items was changed at T2. Before the participants were presented with the items, a definition of phishing was given, to ensure that participants would have a common understanding of this threat. The questions regarding behavioural intention and online information-sharing behaviour included a timeframe of four weeks, since time is an important element of behaviour – in addition to action (not sharing or disclosing), target (personal information) and context (online) (Fishbein & Ajzen, 2010). Accordingly, the post-test was conducted four weeks after the pre-test.

The measures related to online information-sharing behaviour were included in both measurements, thus also prior to the intervention (T1), to assess previous information-sharing behaviour (Milne et al., 2002). This was to address a limitation of PMT studies that assume that end users do not already adopt the target coping response (Tanner, Hunt, & Eppright, 1991). Online information-sharing behaviour was measured by means of self-report. The measures on

resistance and avoidance were also included in both measurements. We added two additional items for avoidance at T2, because according to Witte (1994), although avoidance occurs immediately, delayed measurements are needed to truly assess avoidance patterns.[46]

We also added some supplementary questions, for example, for the purpose of checking validity of the fear appeals (T1). Questions were included to measure message involvement (Shillair et al., 2015) to check whether respondents had read the fear appeal and whether they consider the information as relevant. In addition, information on demographic characteristics, internet experience and phishing awareness were collected. It was sufficient to do this at T1 only because we were able to link the answers of individual participants from both measurements.

Before the data were collected, we conducted a pilot study. First-year bachelor students from NHL University of Applied Sciences who followed courses in research methods were participants. This was to rectify potential problems before the main study was conducted. The pilot study took place in December 2016 and was conducted on paper. In total, 65 students participated in the pilot of which 33 received the strong manipulation and the other 32 the weak manipulation. All students filled out a supplementary questionnaire with 13 items representing PMT's core variables, 4 items measuring fear, 5 items measuring message rejection and 12 questions regarding the validity of the fear appeals, that is message involvement, argument quality (De Hoog et al., 2005), and also issue derogation and perceived manipulation (Witte et al., 1998). With the exception of message involvement, these constructs were only included in the pilot. All measures used a 5-point Likert scale (1 totally disagree – 5 totally agree); see also Appendix V.

The pilot study resulted in a positive evaluation on the fear appeals. In terms of argument quality the strong and weak fear appeal scored reasonably well, respectively 3.7 and 3.5. The mean scores of issue derogation (M = 2.3 in both cases) and perceived manipulation (M = 2.5 and M = 2.2) can be considered good indicators of the fear appeals not being viewed as overblown or misleading. Reliability scores of the variables were adequate, with the exception of message rejection. We made some adjustments regarding the wording of the items and added an item to improve this. Moreover, instead of measuring message rejection as a single construct, we measured it by means of two constructs in the final questionnaire, namely resistance and avoidance.

[46] In the further analysis, we use two avoidance constructs: avoidance (measured at T1) and delayed avoidance (measured at T2). See also Section 9.3.3.

An external recruitment service of online panels handled the sampling procedure of participants of the main study. The participants were randomly assigned to one of the experimental conditions (strong fear appeal, weak fear appeal and control condition). By means of stratified random sampling for each condition, we aimed to recruit a representative sample of the Dutch population (by gender and age). We presented the study to the participants as an investigation of internet users' attitudes and behaviours towards information sharing online and phishing. Anonymity was guaranteed to reduce the likelihood of social desirability in the answers of the participants (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Data collection took place in 2017, between February 28 and March 13 (T1) and the follow-up measurement between April 4 and April 21 (T2). As an incentive, the research participants received for their voluntary participation panel points that can be used for discounts at web shops or for donations to charities.

9.3.2 Participants

In total, 1,219 respondents filled out the questionnaire at T1 and 880 at T2, a retention rate of 72%. We anticipated that fewer participants would partake in the post-test as participation was voluntary. However, measures were taken to enhance the response of the second measurement, for example, by presenting the study as consisting of two parts and by giving participants extra points for their continued participation. The average completion time of the questionnaire for both studies – across the three variants – was 8 minutes and 21 seconds at T1 and 6 minutes and 13 seconds at T2.

Eighteen responses at T1 were excluded from data analysis, reducing the set of respondents to 1,201. One was excluded by means of a registration error (recording their age to be 107), ten because of filling out two variants of the questionnaire, two because they had no reference number for comparisons between the datasets, and five because reliability of their answers was in doubt.[47] For T2, the same procedure was carried out, resulting in the exclusion of ten respondents because of filling out two variants of the questionnaire, seventy-four because they had a reference numbers not occurring in T1[48], one

[47] So-called validator scores (ranging from 0–100) were calculated based on how fast respondents completed the questionnaire, the way grid questions were filled out and how open-ended questions were completed (DataIM, 2008). Scores lower than 50 were closely examined which resulted in leaving participants out when scores were 40 or below. In general, these respondents filled out the questionnaire in just two minutes and/or mostly filled out the neutral option in the grid questions.

[48] These participants were able to participate in T2 due to an error in the invitation process for T2. So-called screen-outs – people that had visited the questionnaire in T1, but could

because of a missing reference number and twelve responses due to doubtful reliability. Thus, the net response frequency was reduced to 786, with a net retention rate of 65%. The participant characteristics for each measurement are enclosed in Table 9.1.

Table 9.1: Descriptive statistics

	Time 1 (N = 1,201)		Time 2 (N = 786)	
	Count	Percentage	Count	Percentage
Gender				
Female	608	50.6	382	48.6
Male	593	49.4	404	51.4
Age[a]				
18–34 years	333	27.7	182	23.2
35–49 years	334	27.8	218	27.7
≥50 years	534	44.5	386	49.1
Education				
Low	151	12.6	110	14.0
Medium	421	35.1	263	33.5
High	629	52.4	413	52.5
Work status				
Employed	674	56.1	444	56.5
Not-employed	527	43.9	342	43.5

[a]*Age distribution T1 (M = 47.65, SD = 16.21); T2 (M = 49.54, SD = 15.83). The age range was in both measurements 19–76 years.*

We compared our figures (T1) with those of the Dutch population in 2016, as measured by Dutch Statistics' Statline. The gender distribution did not deviate from the Dutch population (χ^2 [1, 1200] = 0.30; p = .863) (Statline, 2017c). Considering age, our sample deviates slightly from the Dutch population (χ^2 [2, 1199] = 6.10; p = .047), with the age group of 40–64 years being somewhat under represented (Statline, 2017c). The age groups that we tested for this comparison were 20–39 (in which we included eleven 19-year olds), 40–64 and 65–80 years. Note that this categorization (from Statline) differs from the one presented in Table 1 (from the response panel). The levels of education differed significantly (χ^2 [2, 1199] = 387.70; p < .001), with the lowest level of education being largely under represented and the highest level of education being largely over represented in our dataset (Statline, 2017b). Regarding work status, participants were more likely to belong to the working population and less likely to the non-working population than the Dutch population (χ^2 [1, 1200] = 54.48; p < .001) (Statline, 2017a). We found no significant differences for demographics between the three measurement groups, in both T1 and T2.

not complete it because the questionnaire had enough participants for certain stratifications – were erroneously also invited for Time 2 (N = 128).

In addition, based on the measurements at T1 (N = 1,201) , the participants can be considered experienced internet users, with two-thirds having used it over 15 years (62.9%) and using it for more than 10 hours a week (64.0%). Additionally, 70.1% agreed or largely agreed to the statement that they were experienced internet users. Participants reported to have a rather good understanding of phishing. Three in five (60.1%) claimed to know what phishing is and what can be done to prevent victimization and over a quarter (27.8%) also asserted to know what it entails, but was not sure what can be done against it. One in ten (10.1%) had heard of it, but did not fully understand the details and 2.0% was unaware of its existence. Finally, participants filled out a statement on whether they themselves are primarily responsible for their online safety. Of the participants, 81.2% have agreed or fully agreed with this statement. A neutral opinion was expressed by 11.2% and 7.7% did not (at all) agree.

9.3.3 Data analysis, validity and reliability

The robustness of the data is tested with reflective and formative measurement models (Hair, Hult, Ringle, & Sarstedt, 2014). Note that the measurement models are tested with T1 data of both experimental conditions (N = 512), excluding the data of the control condition (N = 274). The rationale for this is that the control condition did not contain data on the resistance and avoidance constructs. Exceptions are the two items representing the delayed avoidance construct (AV4 and AV5), which were measured at T2 only.

Component loadings of the individual items, except three items of the avoidance construct, loaded highly (≥ .70) on the corresponding component, providing evidence for uni-dimensionality of the items. However, we had to remove one item of protection motivation (PM3), because this item loaded high on self-efficacy as well (see Table 9.2).

Instead of using one avoidance construct, we continue with two avoidance constructs, i.e., avoidance and delayed avoidance. We made this distinction guided by (a) the results the full measurement model and (b) because the avoidance construct contained items measured at two different data collection moments (T1 [AV1, AV2, AV3] and T2 [AV4, AV5]), as was suggested by Witte (1994). The item AV2 needed to be removed because it loaded too low on its construct (< .70). The final measurement model (excluding PM3 and AV2) is presented in Table 9.3.

Table 9.2: Full measurement model (N = 512)

	PV	PS	FE	RE	SE	RC	AT	PM	RS	AV
PV1	**0.91**	0.15	0.48	-0.10	-0.09	0.38	0.01	0.04	-0.09	0.36
PV2	**0.86**	0.16	0.39	0.00	-0.09	0.32	0.00	0.02	-0.11	0.30
PV3	**0.90**	0.13	0.49	-0.05	-0.13	0.44	0.01	0.01	-0.07	0.42
PS1	0.13	**0.88**	0.31	0.19	0.15	0.04	0.21	0.22	-0.19	0.10
PS2	0.15	**0.93**	0.37	0.20	0.13	0.08	0.22	0.26	-0.20	0.13
PS3	0.16	**0.92**	0.40	0.20	0.11	0.13	0.20	0.21	-0.23	0.12
FE1	0.40	0.37	**0.88**	0.07	0.02	0.32	0.18	0.18	-0.15	0.42
FE2	0.41	0.38	**0.91**	0.07	-0.01	0.38	0.18	0.15	-0.16	0.43
FE3	0.52	0.35	**0.92**	0.02	-0.02	0.36	0.16	0.16	-0.18	0.41
FE4	0.52	0.35	**0.91**	0.04	-0.03	0.37	0.18	0.14	-0.18	0.41
RE1	-0.04	0.15	0.01	**0.74**	0.26	-0.05	0.19	0.22	-0.22	-0.07
RE2	-0.02	0.13	0.08	**0.80**	0.36	-0.06	0.26	0.35	-0.24	0.00
RE3	-0.08	0.23	0.03	**0.86**	0.36	-0.10	0.34	0.34	-0.24	-0.02
SE1	0.05	0.24	0.13	0.48	**0.84**	-0.19	0.42	0.64	-0.30	0.14
SE2	-0.19	0.03	-0.10	0.29	**0.89**	-0.46	0.38	0.59	-0.24	-0.01
SE3	-0.16	0.09	-0.06	0.32	**0.90**	-0.47	0.45	0.69	-0.27	0.01
RC1	0.23	0.03	0.17	-0.15	-0.51	**0.72**	-0.29	0.14	0.14	0.09
RC2	0.35	0.07	0.37	-0.04	-0.22	**0.77**	-0.05	0.05	0.05	0.35
RC3	0.35	0.15	0.37	-0.04	-0.28	**0.81**	-0.03	0.00	0.00	0.29
RC4	0.40	0.05	0.32	-0.07	-0.32	**0.82**	-0.12	0.10	0.10	0.34
AT1	0.00	0.20	0.16	0.33	0.42	-0.11	**0.88**	0.50	-0.30	0.17
AT2	-0.01	0.20	0.14	0.28	0.42	-0.16	**0.86**	0.46	-0.29	0.13
AT3	0.00	0.18	0.18	0.26	0.40	-0.14	**0.90**	0.46	-0.27	0.17
AT4	0.04	0.23	0.20	0.36	0.43	-0.12	**0.88**	0.51	-0.34	0.16
AT5	0.01	0.20	0.18	0.28	0.45	-0.17	**0.92**	0.51	-0.33	0.18
PM1	0.02	0.23	0.17	0.33	0.59	-0.13	0.48	**0.88**	-0.39	0.15
PM2	0.02	0.23	0.17	0.35	0.66	-0.21	0.48	**0.93**	-0.43	0.17
PM3	0.00	0.18	0.13	0.33	0.72	-0.25	0.50	**0.91**	-0.42	0.21
PM4	0.05	0.27	0.16	0.41	0.69	-0.18	0.53	**0.92**	-0.41	0.20
RS1	-0.07	-0.21	-0.17	-0.27	-0.29	0.11	-0.35	-0.38	**0.85**	0.02
RS2	-0.06	-0.13	-0.13	-0.26	-0.27	0.06	-0.29	-0.44	**0.83**	-0.07
RS3	-0.12	-0.23	-0.16	-0.16	-0.18	0.05	-0.17	-0.25	**0.73**	0.11
AV1	0.28	0.02	0.27	-0.06	-0.06	0.35	-0.01	0.00	0.17	**0.63**
AV2	0.20	0.12	0.27	0.08	0.15	0.14	0.18	0.23	-0.04	**0.59**
AV3	0.23	0.03	0.25	-0.07	-0.06	0.27	0.01	0.01	0.18	**0.63**
AV4	0.34	0.12	0.38	-0.03	0.08	0.23	0.21	0.22	-0.11	**0.79**
AV5	0.34	0.14	0.39	-0.02	0.07	0.21	0.22	0.21	-0.11	**0.79**

Note. PV: perceived vulnerability; PS: perceived severity; FE: Fear; RE: response efficacy; SE: self-efficacy; RC: response costs; AT: attitude; PM: protection motivation; RS: Resistance; AV: Avoidance.

Table 9.3: Final measurement model (N = 512)

	PV	PS	FE	RE	SE	RC	AT	PM	RS	AV	AVd
PV1	**0.91**	0.15	0.48	-0.10	-0.09	0.38	0.01	0.04	-0.09	0.24	0.33
PV2	**0.86**	0.16	0.39	0.00	-0.09	0.32	0.00	0.02	-0.11	0.22	0.27
PV3	**0.90**	0.13	0.49	-0.05	-0.12	0.44	0.01	0.02	-0.07	0.31	0.34
PS1	0.13	**0.88**	0.31	0.19	0.15	0.04	0.21	0.23	-0.19	0.00	0.12
PS2	0.15	**0.93**	0.37	0.20	0.13	0.08	0.22	0.27	-0.21	0.03	0.13
PS3	0.16	**0.92**	0.40	0.20	0.11	0.13	0.20	0.22	-0.23	0.04	0.12
FE1	0.40	0.37	**0.88**	0.07	0.02	0.33	0.18	0.19	-0.15	0.30	0.34
FE2	0.41	0.38	**0.91**	0.07	-0.01	0.38	0.18	0.16	-0.16	0.27	0.37
FE3	0.52	0.35	**0.92**	0.02	-0.02	0.36	0.16	0.17	-0.18	0.25	0.37
FE4	0.52	0.35	**0.91**	0.04	-0.03	0.37	0.18	0.14	-0.18	0.27	0.37
RE1	-0.04	0.15	0.01	**0.74**	0.26	-0.05	0.19	0.24	-0.22	-0.11	-0.04
RE2	-0.02	0.13	0.08	**0.80**	0.36	-0.06	0.26	0.35	-0.24	-0.05	0.01
RE3	-0.08	0.23	0.03	**0.85**	0.36	-0.10	0.34	0.34	-0.24	-0.04	-0.04
SE1	0.05	0.24	0.13	0.48	**0.84**	-0.18	0.42	0.63	-0.30	0.02	0.15
SE2	-0.19	0.03	-0.10	0.29	**0.89**	-0.46	0.39	0.56	-0.24	-0.09	0.01
SE3	-0.16	0.09	-0.06	0.32	**0.90**	-0.46	0.45	0.65	-0.27	-0.10	0.04
RC1	0.23	0.03	0.17	-0.14	-0.51	**0.71**	-0.29	-0.32	0.14	0.17	0.04
RC2	0.35	0.07	0.37	-0.04	-0.22	**0.77**	-0.05	-0.05	0.05	0.31	0.25
RC3	0.35	0.15	0.37	-0.04	-0.28	**0.81**	-0.03	-0.07	0.00	0.30	0.19
RC4	0.40	0.05	0.32	-0.07	-0.32	**0.82**	-0.12	-0.14	0.10	0.33	0.24
AT1	0.00	0.20	0.16	0.33	0.42	-0.11	**0.88**	0.48	-0.30	-0.02	0.21
AT2	-0.01	0.20	0.14	0.28	0.42	-0.16	**0.86**	0.46	-0.28	0.00	0.15
AT3	0.00	0.18	0.18	0.26	0.40	-0.13	**0.90**	0.45	-0.27	0.00	0.21
AT4	0.04	0.23	0.20	0.36	0.43	-0.11	**0.88**	0.50	-0.33	0.00	0.19
AT5	0.01	0.20	0.18	0.28	0.45	-0.16	**0.92**	0.50	-0.33	0.00	0.23
PM1	0.02	0.23	0.17	0.33	0.59	-0.12	0.48	**0.90**	-0.39	-0.01	0.18
PM2	0.02	0.23	0.17	0.35	0.66	-0.20	0.48	**0.93**	-0.43	-0.01	0.21
PM4	0.05	0.27	0.16	0.41	0.69	-0.18	0.53	**0.93**	-0.41	0.02	0.21
RS1	-0.07	-0.21	-0.17	-0.27	-0.29	0.11	-0.35	-0.37	**0.85**	0.15	-0.07
RS2	-0.06	-0.13	-0.13	-0.26	-0.27	0.06	-0.29	-0.43	**0.83**	0.13	-0.17
RS3	-0.12	-0.23	-0.16	-0.16	-0.18	0.05	-0.17	-0.25	**0.74**	0.21	-0.01
AV1	0.28	0.02	0.27	-0.06	-0.06	0.35	-0.01	0.00	0.17	**0.88**	0.24
AV3	0.23	0.03	0.25	-0.07	-0.06	0.27	0.01	0.00	0.18	**0.85**	0.24
AV4	0.34	0.12	0.38	-0.03	0.08	0.23	0.21	0.21	-0.11	0.26	**0.96**
AV5	0.34	0.14	0.39	-0.02	0.07	0.21	0.22	0.20	-0.10	0.27	**0.96**

Note. PV: perceived vulnerability; PS: perceived severity; FE: Fear; RE: response efficacy; SE: self-efficacy; RC: response costs; AT: attitude; PM: protection motivation; RS: Resistance; AV: Avoidance; AVd: Delayed avoidance.

Convergent validity was analysed using the average variance extracted (AVE) by a construct from its indicators, which should be 0.70 or higher (Henseler, Ringle, & Sinkovics, 2009). Except response efficacy (AVE = 0.64), response costs (AVE = 0.61) and resistance (AVE = 0.65), all values exceeded this cut-off point. Because the AVE values of these three constructs still exceeded 0.50, they were retained in their current form, because more variability in the items of these constructs was accounted for by its component than was not. Construct reliability was assessed using the composite reliability co-efficient. All constructs showed good reliability (≥ .84).

Discriminant validity was positively evaluated according the Fornell-Larcker-criterion. This holds that the square root of AVE by each construct from its indicators was greater than its correlation with the remaining constructs (see

Table 9.4). Finally, no multicollinearity issues were observed when testing for this in SPSS; tolerance values were well above 0.10 and VIF values were well below 10.

Table 9.4: Coefficients of discriminant validity (N = 512)

	PV	PS	FE	RE	SE	RC	AT	PM	RS	AV	AVd
PV	0.89										
PS	0.16	0.91									
FE	0.51	0.40	0.91								
RE	-0.06	0.22	0.05	0.80							
SE	-0.12	0.14	-0.01	0.42	0.87						
RC	0.43	0.10	0.40	-0.09	-0.42	0.78					
AT	0.01	0.23	0.19	0.34	0.48	-0.15	0.89				
PM	0.03	0.27	0.18	0.40	0.70	-0.18	0.54	0.92			
RS	-0.10	-0.23	-0.19	-0.29	-0.31	0.09	-0.34	-0.44	0.81		
AV	0.29	0.03	0.30	-0.08	-0.07	0.36	-0.01	0.00	0.20	0.87	
AVd	0.35	0.13	0.40	-0.03	0.08	0.23	0.22	0.22	-0.11	0.28	0.96

Note. Off-diagonal values are correlations. Diagonal values are square root of average extracted variances. PV: perceived vulnerability. PS: perceived severity. FE: fear. RE: response efficacy. SE: self-efficacy. RC: response costs. AT: attitude. PM: protection motivation. RS: resistance. AV: Avoidance. AVd: Delayed avoidance.

We used SPSS (version 23) for conducting analysis of variance (ANOVA). First, we used one-way between-groups ANOVA to determine the mean differences on the dependent variables across the three different groups (T1). Additional post-hoc tests were used to determine where the differences occurred. Second, we used a mixed-measures ANOVA to determine whether the effect of fear appeals is stable over time (T2 in comparison with T1). These analyses were to answer Research Questions 2-5.

Third, we used the PROCESS macro for SPSS (Hayes, 2016) to conduct multi-categorical mediation analyses (Hayes & Preacher, 2014). Mediation analysis provides information on how effects occur (Hayes, 2014). The idea of mediation in this study is to determine if the effect of the manipulation at T2 runs through the effect at T1. It answers the question whether the effect at T1 is the reason for the effect at T2. If this is not the case (i.e., when a non-significant indirect effect is found), then the effect at T2 cannot be attributed to the effect at T1. We tested this for outcome variables attitude and protection motivation and the predictor variables that were included in the fear appeals: perceived vulnerability, perceived severity, response efficacy and self-efficacy. This type of analysis provides additional evidence for answering Research Question 5.

Fourth, a Kruskal-Wallis test was used to investigate the difference in online information-sharing behaviour across the three conditions for T2, providing an answer to Research Question 6.

9.4 Results

Before presenting the results of the one-way between-groups ANOVA, the mixed-measures ANOVA and mediation analysis, we first analyse the participants' internet behaviour.

9.4.1 Internet and online information sharing behaviour

We asked the participants on a dichotomous scale (yes/no) whether they made use of the following six online services (T1, N = 1,201): e-mail (99.8%); online banking (96.7%); buying products on online marketplaces and/or web shops (93.7%); instant messaging (e.g., WhatsApp and Facebook Messenger) (87.1%); social media (e.g., Facebook, Instagram and LinkedIn) (84.4%); and selling products on online marketplaces and/or web shops (57.8%).

Next, we asked participants to indicate to what extent they had shared six types of personal information online in the previous year (see Table 9.5) and in the previous month. The participants were told beforehand that online information sharing can be done both actively (e.g., through social media and e-mail) and passively (e.g., by including contact information on a personal website or on a public social media profile). Here, information-sharing does not include activities such as logging in to an e-mail account or online banking environment.

Table 9.5: Online information sharing behaviour in the previous year (N = 1,201)

	No	Once	More than once	Do not know
E-mail address	14.7	29.6	52.8	2.8
Home address	37.4	36.1	22.5	4.1
Bank account number	58.8	27.7	11.1	2.4
Citizen service number	79.1	16.8	1.7	2.4
Log-in credentials	92.9	2.7	1.7	2.6
PIN codes / security codes	96.2	1.2	0.6	2.1

Of the 990 participants who had shared their e-mail address, 71.7% indicated to have done this at least once in the previous month. Of the 703 participants who had shared their physical address the figure was 61.6%. Bank account number was shared in the previous month at least once by 53.7% of 466 participants and the citizen service number by 44.1% of 222 participants. The 54 participants, who had shared their log-in credentials in the previous year, had done this in 53.7% of the cases at least once in the previous month. Finally, of the 21 participants who had shared their PIN codes and/or security codes at least once in the previous year, 57.2% had done this in the previous month. In total, 180 participants (15.5%) indicated that they did not share any of the requested information online in the previous year, rising to 411 (34.2%) for sharing in the previous month.

We were also interested in how participants shared their personal information online. They could choose from multiple pre-determined methods (N = 1,021): by e-mail (62.7%); on web shops (47.9%); on websites (e.g., to register, to receive a discount, to download a file or to get a prize) (28.9%); by instant messaging (26.4%); on corporate websites (9.3%); by social media messages (6.2%); on personal websites/social media profiles (5.1%); and other (5.3%).

The final step regarding sharing personal information online was to check with the participants to what extent they had done so on trustworthy locations or to trustworthy parties. These results apply to active information-sharing only. Because participants could have shared their information to both familiar and unfamiliar sources the percentages presented next do not precisely add up to 100. Those who had shared personal information online by means of e-mail (N = 660), 75.8% indicated to had sent it to someone they knew personally and 28.5% to have sent it to someone they do not know personally. Of the participants who had shared their details on web shops (N = 489), 40.7% had done this on those they were familiar with and 62.4% on web shops they were not familiar with. For websites (N = 295), the figures were 34.6% and 70.2%. Regarding sharing personal information via instant messaging (N = 270) and social media messages (N = 63), 94.4% and 82.5% (respectively) did this with people they were well familiar with and 7.4% and 23.8% (respectively) with people they were not familiar with.

9.4.2 The effect of fear appeals on outcomes

The participants in the fear appeal conditions were asked about their message involvement – after completing the PMT-items. In the strong-fear appeal condition (N = 249), 69.9% (strongly) agreed to the statement of having carefully read the fear appeal message. In the weak fear appeal (N = 263), this percentage was 73.0. Respectively 18.1% and 19.0% were neutral and 12.0% and 8.0% (strongly) disagreed with this statement. The second statement regarding message involvement was 'the text contains relevant information for me'. In the strong fear appeal, 49.3% (strongly) agreed, 34.9% was neutral and 15.7% (strongly) disagreed with this statement. For the weak fear appeal, these numbers were respectively 50.2%, 33.1% and 16.7%. Considering message involvement, *t*-tests showed no significant differences between both fear appeal conditions.

A one-way between-groups ANOVA was conducted to explore the impact of fear appeals on cognitions, attitude and online behavioural intentions at T1. Note that the results represent only those respondents who completed both questionnaires (N = 786). First, we checked if the assumption of homogeneity was not violated. This was not the case, because the Levene's test produced

results well above the threshold of .05. Although significant effects are visible between the conditions (see Table 9.6), the actual difference in the mean scores is quite small for all variables. Indeed, the effect sizes, calculated using partial eta squared, were small: η_p^2 = .02 for self-efficacy, .01 for perceived vulnerability, response efficacy, attitude and protection motivation and < .01 for the remaining variables. Effect sizes are interpreted according to Cohen's (1988) classification scheme (i.e., .01 = small; .06 = medium; .14 = large).

Table 9.6: Results from one-way between groups ANOVA (N = 786)

Constructs	*F (2, 783)*	*p*	η_p^2		Mean, *SD*
Perceived vulnerability	4.39	.013	.01	0)	2.54, .74
				1)	2.40, .76
				2)	2.60, .85
Perceived severity	1.73	.178	.00	0)	3.58, .81
				1)	3.68, .78
				2)	3.70, .77
Fear	0.68	.509	.00	0)	2.85, .94
				1)	2.79, .97
				2)	2.88, .95
Response efficacy	3.74	.024	.01	0)	3.70, .75
				1)	3.83, .71
				2)	3.86, .75
Self-efficacy	7.49	.001	.02	0)	3.26, .94
				1)	3.51, .84
				2)	3.52, .88
Response costs	1.06	.347	.00	0)	2.98, .84
				1)	2.88, .83
				2)	2.95, .86
Attitude	5.64	.004	.01	0)	3.60, .81
				1)	3.79, .80
				2)	3.82, .80
Protection motivation	5.96	.003	.01	0)	3.34, .95
				1)	3.57, .93
				2)	3.59, .94

Note. 0: control condition. 1: weak fear appeal. 2: strong fear appeal.

There were significant differences between the conditions on perceived vulnerability, response efficacy, self-efficacy, attitude and protection motivation. Post-hoc comparisons using the Tukey HSD test indicated that the higher mean scores for the strong fear appeal on perceived vulnerability differed significantly from the weak fear appeal (p < .05); the control condition did not differ significantly from either fear appeal conditions. With regard to response efficacy, the higher mean of the strong fear appeal differed significantly from that of the control condition (p < .05); the weak fear appeal did not differ significantly from the other two conditions. Considering self-efficacy, the lower mean score of control condition differed significantly (p < .01) from that of the strong fear appeal and weak fear appeal; the fear appeal conditions did not differ

significantly from each other. A similar pattern was noticeable for attitude and protection motivation. In both instances the mean score of the control condition was significantly lower than the mean scores of the strong fear appeal ($p < .01$) and the weak fear appeal ($p < .05$).

We conducted a mixed-measures ANOVA to explore whether the effect of fear appeals was stable over time (see Table 9.7). The main effect of condition was significant for self-efficacy, attitude and protection motivation and marginally significant for response efficacy. There was a positive small effect of time on most dependent variables and a moderate effect on others (attitude and perceived vulnerability), but not on fear and protection motivation. Only for perceived vulnerability was the main effect of time qualified by a significant interaction effect. This main effect was moderate for weak fear appeal ($d = .31$), small for the control condition ($d = .20$) and very small for strong fear appeal ($d = .09$).

Table 9.7: Results from a mixed-measures ANOVA (N = 786)

Constructs		*F (df)*		*p*	η_p^2		M (*SD*) (T1)	M (*SD*) (T2)
Perceived vulnerability	C	(2, 783) =	2.00	.136	.01	0)	2.54 (.74)	2.68 (.76)
	T	(1, 784) =	39.95	< .001	.05	1)	2.40 (.76)	2.64 (.79)
	T*C	(2, 783) =	3.70	.025	.01	2)	2.60 (.85)	2.68 (.85)
Perceived severity	C	(2, 783) =	0.77	.462	.00	0)	3.58 (.81)	3.70 (.78)
	T	(1, 784) =	5.12	.024	.01	1)	3.68 (.78)	3.70 (.76)
	T*C	(2, 783) =	1.49	.225	.00	2)	3.70 (.77)	3.73 (.75)
Fear	C	(2, 783) =	0.28	.756	.00	0)	2.85 (.94)	2.85 (.94)
	T	(1, 784) =	1.50	.220	.00	1)	2.79 (.97)	2.80 (.97)
	T*C	(2, 783) =	1.65	.192	.00	2)	2.88 (.95)	2.78 (1.01)
Response efficacy	C	(2, 783) =	2.53	.081	.01	0)	3.70 (.75)	3.85 (.75)
	T	(1, 784) =	14.11	< .001	.02	1)	3.83 (.71)	3.95 (.69)
	T*C	(2, 783) =	2.78	.062	.01	2)	3.86 (.75)	3.86 (.78)
Self-efficacy	C	(2, 783) =	5.36	.005	.01	0)	3.26 (.94)	3.42 (.94)
	T	(1, 784) =	7.29	< .010	.01	1)	3.51 (.84)	3.59 (.86)
	T*C	(2, 783) =	2.76	.064	.01	2)	3.52 (.88)	3.52 (.92)
Response costs	C	(2, 783) =	0.99	.373	.00	0)	2.98 (.84)	2.86 (.88)
	T	(1, 784) =	18.45	< .001	.02	1)	2.88 (.83)	2.78 (.80)
	T*C	(2, 783) =	0.13	.880	.00	2)	2.95 (.86)	2.82 (.98)
Attitude	C	(2, 783) =	6.71	.001	.02	0)	3.60 (.81)	3.82 (.89)
	T	(1, 784) =	59.11	< .001	.07	1)	3.79 (.80)	4.03 (.83)
	T*C	(2, 783) =	0.14	.866	.00	2)	3.82 (.80)	4.02 (.88)
Protection motivation	C	(2, 783) =	4.41	.012	.01	0)	3.34 (.95)	3.44 (1.03)
	T	(1, 784) =	1.31	.252	.00	1)	3.57 (.93)	3.63 (.98)
	T*C	(2, 783) =	2.39	.092	.01	2)	3.59 (.94)	3.53 (1.03)

*Note. C: condition. T: time. T*C: time × condition. 0: control condition. 1: weak fear appeal. 2: strong fear appeal.*

Any differences between the two fear appeal conditions on message rejection variables were small: resistance (T1; strong fear appeal, M = 2.4, *SD* = .79; weak fear appeal, M = 2.4, *SD* = .80), avoidance (T1; strong fear appeal, M = 2.6, *SD* = .91; weak fear appeal, M = 2.5, *SD* = .87), and delayed avoidance

(T2; strong fear appeal, M = 2.1, *SD* = .98; weak fear appeal, M = 2.2, *SD* = .94). The *t*-tests showed no significant differences between both fear appeal conditions for these three variables, with effect sizes *d* = 0.00, 0.08, and 0.10, respectively.

9.4.3 Mediation analysis

Multi-categorical mediation analyses were conducted to test the outcome variables attitude and protection motivation (T1) as a mediator of attitude and protection motivation (T2), respectively. Because we have three conditions, dummy variables were created (i.e., D_1 represents the weak fear appeal and D_2 the strong fear appeal, both in comparison with the control condition). Figures 9.1–9.2 present the results of mediation analyses.

In the first two analyses (Figure 9.1/9.2), the experimental condition was significant as an indirect positive predictor of attitude/protection motivation (T2), mediated by attitude/protection motivation (T1). However, experimental condition was not significant as a direct predictor of attitude (T2). According to the decision tree of Zhao, Lynch, and Chen (2010), these results can be interpreted as indirect-only mediation.

Figure 9.1: Model of fear appeal condition as a predictor of attitude (T2) mediated by attitude (T1).

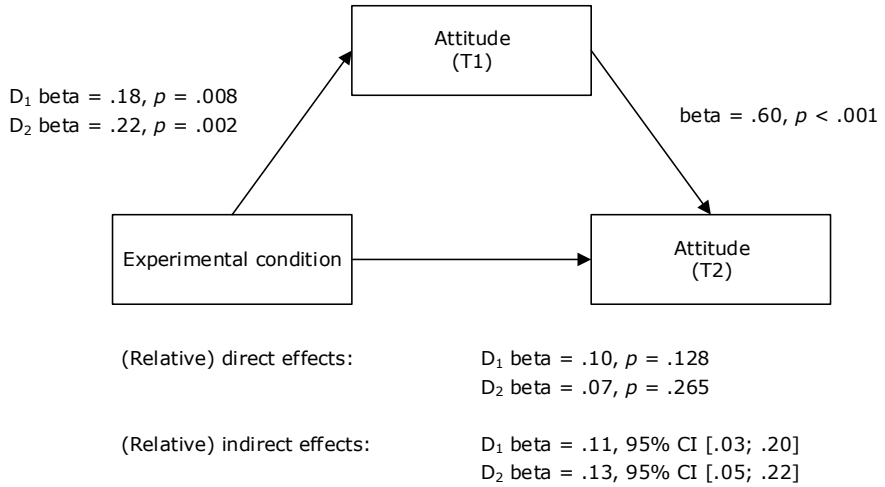
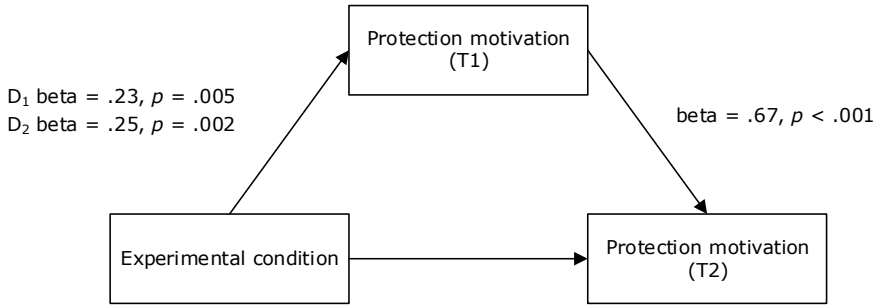


Figure 9.2: Model of fear appeal condition as a predictor of protection motivation (T2) mediated by protection motivation (T1).

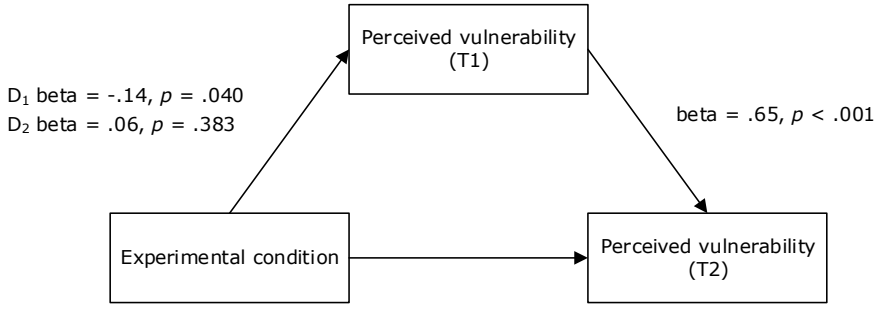


(Relative) direct effects: D_1 beta = .04, p = .576; D_2 beta = -.07, p = .288

(Relative) indirect effects: D_1 beta = .16, 95% CI [.05; .27]; D_2 beta = .17, 95% CI [.06; .29]

We also conducted mediation analysis for the cognition variables present in the fear appeals (Figures 9.3-9.6). This is important because the mixed-measures ANOVA is only useful to demonstrate any potential interaction effect between time and condition. However, unlike the mediation analysis, this does not address the effect of the manipulation at T2 with the measurement at T1 held constant and as a potential mediator.

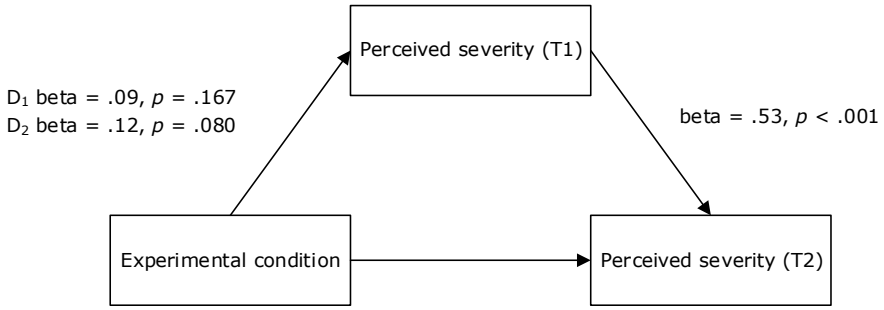
Figure 9.3: Model of fear appeal condition as a predictor of perceived vulnerability (T2) mediated by perceived vulnerability (T1).



(Relative) direct effects: D_1 beta = .05, p = .370; D_2 beta = -.04, p = .435

(Relative) indirect effects: D_1 beta = -.09, 95% CI [-.17; -.01]; D_2 beta = .04, 95% CI [-.05; .13]

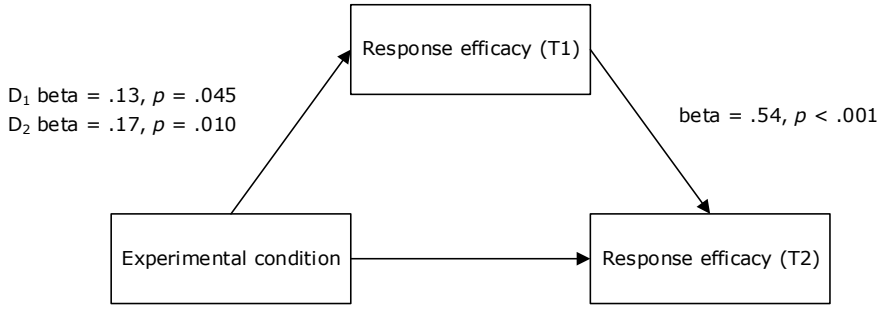
Figure 9.4: Model of fear appeal condition as a predictor of perceived severity (T2) mediated by perceived severity (T1).



(Relative) direct effects: D_1 beta = -.05, p = .353; D_2 beta = -.04, p = .494

(Relative) indirect effects: D_1 beta = .05, 95% CI [-.02; .12]; D_2 beta = .06, 95% CI [-.01; .14]

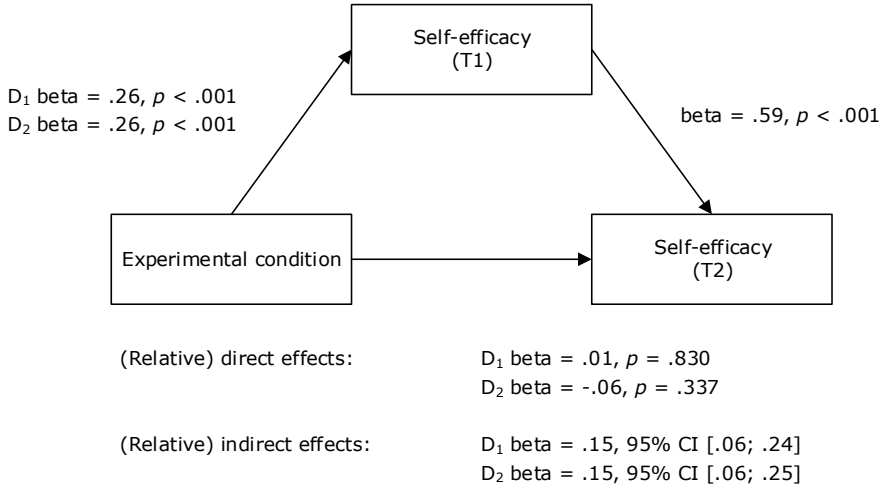
Figure 9.5: Model of fear appeal condition as a predictor of response efficacy (T2) mediated by response efficacy (T1).



(Relative) direct effects: D_1 beta = .04, p = .500; D_2 beta = -.06, p = .266

(Relative) indirect effects: D_1 beta = .07, 95% CI [.00; .14]; D_2 beta = .09, 95% CI [.02; .16]

Figure 9.6: Model of fear appeal condition as a predictor of self-efficacy (T2) mediated by self-efficacy (T1).



We observe that, similar to attitude and protection motivation, experimental condition was significant as an indirect positive predictor of the coping variables response efficacy and self-efficacy (T2), mediated by respectively response efficacy and self-efficacy (T1), see Figures 9.5-9.6. Furthermore, experimental condition was not significant as a direct predictor in both cases. Thus, these results can be interpreted as indirect-only mediation.

The results from mediation analysis regarding the threat variables perceived vulnerability and perceived severity were less clear, because the lower limits and upper limits included the number of zero in three of four instances, see Figures 9.3-9.4. This corresponds with a non-significant test result. However, for perceived vulnerability the relative indirect effects of condition (strong fear appeal versus control) was different from zero, which supports the conclusion that M (perceived vulnerability T1) mediates the effect of X (experimental condition) on Y (perceived vulnerability T2) (Hayes & Preacher, 2014).

9.4.4 Effects on online information-sharing behaviour

Finally, we tested if there was a difference in online information-sharing behaviour across the three conditions at T2. A Kruskal-Wallis test showed no significant effect of intervention (strong fear appeal, N = 249, weak fear appeal, N = 263 and control, N = 274), χ^2 (2, 786) = 1.14, η_p^2 = 0.00, p = .567. Moreover, more than half of all the participants (58.1%) indicated to have shared their personal information both a month prior to T1 and a month prior to T2.

We also tested the level of variance explained for online information-sharing behaviour – using logistic regression. Predictor variables were protection motivation and previous online information-sharing behaviour.[49] The likelihood ratio (R^2_L) is around .10 in all three conditions.[50] We find that previous behaviour better predicts behaviour than intentions do in all three conditions. Only in the strong-fear appeal condition was protection motivation a marginally significant predictor of actual behaviour (p = .085).

9.5 Conclusion and discussion

We first answer Research Question 1: To what extent do end users share their personal information online? Based on the data gathered at T1, it became clear that the participants often share their personal information online. This primarily goes for address details, which is unsurprising since people need to find each other in this way, especially on the internet. More sensitive data are shared to a lesser extent, that is bank account numbers and citizen service numbers. Again, these are often necessary for instance to buy products or to make use of governmental services. However, it also became clear that respondents share log-in credentials (4.4%) and PIN codes or security codes (1.8%). It could be that participants have not properly read the instructions before answering this question, but these results indicate that a number of participants engage in potentially harmful online behaviour. This is also true for participants that share these and other personal information on unfamiliar online locations or to unfamiliar parties or individuals, which commonly occurred.

Next, we turn to answering Research Question 2: What effect do fear appeals have on end-users' cognitions? We observed from the one-way between-groups ANOVA that the strong-fear appeal message provided highest mean scores for all predictor variables. The exception was response costs, as predicted, because response costs were not explicitly addressed within the messages, so an effect might not be expected indeed.[51] The scores were, however, only significant for

[49] Only online information-sharing behaviour in the previous month (measured at T1) was used as an additional explanatory variable for online information-sharing behaviour (measured at T2), because the correlation was well above the threshold of .10. Other potential predictor variables, i.e., demographic variables, internet experience, knowledge on phishing and level of responsibility did not meet this criterion.

[50] For the strong fear appeal and weak fear appeal conditions, we tested whether the explained variance for behaviour would increase when adding the message rejection variables as additional explanatory variables for self-reported online information-sharing behaviour (measured at T2). This was, however, not the case as it only increased by one hundredth. Only delayed avoidance was a marginally significant predictor of not sharing personal information online (beta = .37, p = .053).

[51] Response costs were tested to determine specificity.

perceived vulnerability in comparison with the weak fear appeal, and for response efficacy and self-efficacy in comparison with the control condition. These results imply that end-users' cognitions can be elevated by means of a fear appeal message, especially when strong arguments are used.

Research Questions 3 and 4 were formulated as follows. What effect do fear appeals have on end-users' (a) attitudes towards precautionary online, and (b) precautionary online behavioural intentions? Again the strong fear appeal produced the highest scores. However, note that the scores were significantly higher only in comparison with the control condition, not the weak fear appeal. This implies that attitudes and behavioural intentions can be raised by making internet users aware of threats and simultaneously providing behavioural advice on how to mitigate these. Protection motivation was heightened, while perceived vulnerability was low, which is a central indicator for personal relevance, and thus an important aspect for how a message is processed. However, according to De Hoog et al. (2007), individuals might still have processed the fear appeal message systematically, because the threat was depicted as severe. They continue by explaining that individuals might find it useful to be well informed, even when the threat is not imminent.

Besides examining protection motivation (danger control), we also looked at three types of fear control (resistance and two avoidance constructs). These constructs were scored low. This is probably due to the low scores on fear as well. Lazarus and Folkman (1984) stress that emotion-focused forms of coping – where fear control can be placed under – tend to be adopted when threat or fear levels are perceived to be high.

We now examine the extent to which the effect of fear appeals was stable over time (Research Question 5). We answer this question first by examining the results from the mixed-measures ANOVA. The results show significant differences in overall mean scores between T1 and T2 for all constructs, except fear and protection motivation. All differences were in the positive direction. Most improvement is found for the constructs perceived vulnerability and attitude. Perhaps, the participants gave the topic at hand (phishing-related security) some thought or spoke about it with others. As a result, they may have realised that one is at risk for falling for phishing scams and sharing personal information online poses avoidable dangers. This positive effect might also be explained by the possibility that filling out a questionnaire such as this one has an awareness-raising effect, since the scores of the control condition were also higher.

The second part of our answer to Research Question 5 is from the results from the mediation analyses. The mediation analyses showed that the fear appeal messages had a significant indirect effect on the second measurement (T2) of outcome variables attitude and protection motivation and PMT variables perceived vulnerability, response efficacy and self-efficacy. This means that the effect of fear appeals at T2 can be attributed to its effect already achieved at T1. For perceived severity no significant indirect effect was observed. Similar to previous studies, the threat-specific variables provide some inconsistencies with what the theory would predict (Wall & Buche, 2017).

Finally, we answer Research Question 6: What effect do fear appeals have on end-users' precautionary online information-sharing behaviour? The results from the Kruskal-Wallis Test indicate that there was no such effect. The finding that the effects on subsequent behaviour are minor corresponds with results from previous studies (Floyd et al., 2000; Milne et al., 2000). This finding is also in line with previous research in the information security domain in which it is demonstrated that people's positive attitudes towards information security practices do not always correspond with their actual information security behaviour (Spiekermann, Grossklags, & Berendt, 2001). Perhaps the fear appeals would have had more effect on behaviour if threat was perceived higher (Boss et al., 2015). Furthermore, we find that previous behaviour better predicts behaviour than intentions do, which is also pointed out by Norman, Boer, and Seydel (2005). According to Liang and Xue (2009), people are motivated to repeat previous actions that led to positive outcomes and avoid behaviour that led to negative outcomes.

Moreover, over half of the participants indicated to have shared their personal information online a month prior to both T1 and T2. In addition, Maloney, Lapinski, and Witte (2011) propose that if perceived threat is too low to produce fear, end users will take no action instigated by the fear appeal, which might further explain our finding that behaviour did not follow intentions. This is also illustrated by De Hoog et al. (2007, p. 263) who state '[…], why should anyone invest effort into avoiding a risk, if one does not feel personally at risk?' Follow-up research on fear appeals is needed to find out how behaviour will be impacted when threats do become more personally relevant (i.e., when perceived vulnerability is sufficiently heightened).

A possible limitation here, that might have affected the results, is that the behaviour of interest was phrased generally (i.e., not sharing personal information online). Perhaps this behaviour should have been further specified (e.g., not sharing personal information online on unfamiliar locations or to unfamiliar parties or individuals). However, it should be noted that participants

reported sharing their information with parties that were both trusted and unfamiliar. Therefore, future research is necessary to find out whether fear appeals would truly modify behaviour. In addition, stronger results might have been found if one-off behaviour was investigated, such as installing anti-virus software, than repeated behaviours such as in our study (Tannenbaum et al., 2015).

According to our results, end-users' cognitions can potentially be influenced by means of fear appeals. We use the term 'potential', because although some of the group differences were significant, the effect sizes were small. An explanation might be that phishing is a well-known threat to Dutch internet users and it is common knowledge that vigilance is required when sharing personal information online; therefore, the variation was low between the groups. In addition, more variation might have been found if 7-point scales were used. The use of 5-point scales can therefore be seen as a possible limitation of our study.

Because our study took place within participants' social context, we created a realistic setting in which end users read a fear appeal message and answered questions about their cognitions, attitudes and behaviours. This implies, however, that we could not control for the effect of other messages related to safe online practices which were not part of intervention, but which participants may have encountered in their day-to-day use of the internet. Furthermore, we only tested two fear appeal variants, one with strong arguments and one with weak arguments regarding threat and coping appraisal. Future studies could benefit from testing more variants (e.g., strong threat-weak coping, weak threat-strong coping, threat-only and coping-only alternatives). Another issue that needs to be taken into consideration is that we provided the fear appeals within an experimental setting. In real-world situations, these may receive less attention (Wall & Buche, 2017).

To conclude, we acknowledge the fact that other factors can influence the way people process information, for instance communicator factors, such as source credibility and liking of the communicator (O'Keefe, 2016). Briggs et al. (2016) address this point, stating that messenger effects have often been ignored in the cybersecurity domain. Furthermore, other message factors were not addressed, such as personalisation (Davinson & Sillence, 2010), visual elements and humour (Kirlappos & Sasse, 2012). Hence, factors being relevant to a peripheral route of information-processing (Petty & Cacioppo, 1986) were lacking. Future research could focus on such aspects as well, potentially motivating less security-minded internet users to perform precautionary online behaviour. However, the peripheral route is believed to produce only short-lived effects.

This would imply that interventions targeting this route would need to be repeated continuously. In addition, recipient-related individual-difference factors like self-control were not included, which could also have an influence on the outcomes (Michie et al., 2011). However, these factors were outside the scope of the present investigation.

Concluding remarks

It is important to note that fear appeals are one of several types of intervention to promote security behaviour against phishing to end users. As noted by Maloney et al. (2011), in the domain of health behaviours, fear appeals might not always be the most appropriate means to do so. Nevertheless, this study demonstrated that fear appeals seem to work for the current context, especially for heightening end-user cognitions, attitudes and behavioural intentions. Fear appeal messages using strong arguments seem to be most efficacious overall, which is also highlighted by the study of Boss et al. (2015), but weak arguments still demonstrate efficacy to some extent. Nevertheless, future studies are needed to find out how subsequent behaviour can be improved, as results on this crucial aspect seem to lag behind. Qualitative studies focussing on understanding perceptions and reactions to fear appeals might complement the methods presented in this chapter. Moreover, follow-up studies are needed to critically evaluate how fear appeals affect end users in the information security domain.

GENERAL CONCLUSION AND DISCUSSION

CHAPTER 10

Improving the safety and security of online banking from an end-user perspective

10.1 Introduction

This thesis investigated online banking fraud victimization and precautionary online behaviour. Specifically, human aspects were the focus of this research. Apparently it is easier, cheaper and more successful for criminals to attack end users using psychology rather than the technology surrounding online banking. Hence, even the best security engineers cannot stop end users from giving away their one-time passwords. Therefore, it makes sense to also use psychology to defend against online banking attacks. This is especially the case for attacks using social engineering, but to some extent also for attacks using technical engineering. As will become clear in this chapter, good security is in people's heads. Considering the further digitization of our society and the increasing dependence on information systems, the case is made that people have to 'bend' with these developments and become resilient when online. This is necessary to stop people from 'breaking' and potentially becoming victims of online banking fraud, or cybercrimes in general.

The general conclusions of this thesis are presented in this chapter. The conclusions are linked to the main research questions outlined in Chapter 1. The main research questions are:

1: What are the perceptions of end users on the safety and security of online banking?

2: How can online banking fraud victimization be explained from an end-user perspective?

3: How can precautionary online behaviour of end users be explained and improved?

The research questions are answered in Sections 10.2 to 10.4 respectively and are needed to form an answer to the central question of this thesis: *To what extent can the safety and security of online banking be improved from an end-user perspective?* This chapter continues with the theoretical and practical implications, which are discussed in Section 10.5 and provides an answer to the central question (10.5.5). In Section 10.6, the limitations of the studies are reflected upon. Finally, some concluding remarks are highlighted in Section 10.7.

10.2 What are the perceptions of end users regarding the safety and security of online banking?

The first research question and its sub-questions are answered by means of the survey study on risk perceptions presented in Chapter 2. The first sub-question that was addressed is the following: *1a) What are the perceptions of end users*

regarding threats to online banking? In order to understand how end users react to attacks targeting online banking, it was necessary to investigate how they feel about it. Online banking users do not consider online banking fraud to be a major problem. They estimate the likelihood of falling for fraudulent schemes involving online banking to be low and the chances of others being victimized by these threats to be higher. On the other hand, online banking users do perceive the 'impact' to be high if online banking fraud does occur.

The second sub-question dealt with predictors of perceived risk: *1b) What factors determine end-users' risk perceptions of threats to online banking?* Three factors can be distilled that contribute most to explaining risk perception; these factors correspond with the literature (e.g., Garland, 2003; Griffin, Neuwirth, Dunwoody, & Giese, 2004). The most important factor predicting risk perception is perceived vulnerability or the perceived likelihood of becoming an online banking fraud victim. Secondary determinants of risk perception are perceived severity or the impact of a threat and the levels of trust in online banking. The latter is characterized by a negative relationship. Factors related to direct or indirect experiences with victimization (self, the social environment and the media) and demographic attributes (gender, age, level of education and work status) had almost no influence on risk perception.

The third sub-question was as follows: *1c) To what extent do end users trust online banking?* Based on the survey results, it is fair to say that online banking users, in general, have reasonable levels of trust in online banking. If the levels of trust were divided in high, medium and low, it would translate in two-thirds experiencing high levels of trust in online banking, a quarter having a medium or neutral level of trust and one-in-eight perceiving low levels of trust in online banking.

The final sub-question concerned experiences of end users with online banking fraud: *1d) How are end users confronted with online banking threats?* 'Confronted' is delimited in this thesis to self-experienced victimization, indirect victimization (in the social environment) and having heard about or read stories in the media about online banking fraud victimization. Based on the survey results, it can be concluded that three-quarters of online banking users hear about online banking fraud victimization through media coverage. To a lesser extent, they experience indirect victimization in their social environment. Nearly one-third of end users know someone personally that has been victimized by a phishing and/or a malware attack on online banking. In conclusion, only few (direct) online banking fraud victims could be identified, namely ten phishing and twenty malware victims – in total, 27 individual victims – whilst some 35% had been confronted with phishing attempts on online banking and 15% with

fraudulent attempts using malware. These 27 victims represent 2.3% of the online banking users. This statistic comes as no surprise when compared to figures from Statistics Netherlands (CBS, 2015b), which are similar.

10.3 How can online banking fraud victimization be explained?

The second research question and its sub-questions are answered based on the studies presented in Chapters 3 to 5. These include the case analyses on 600 real-world bank files and the interviews with 30 online banking fraud victims.

The first sub-question that was addressed is the following: *2a) How and why do end users become victims of online banking fraud?* In order to answer this question, case analyses and semi-structured interviews were conducted. At its most basic form, the 'how-question' for phishing victimization can be answered as follows: end users give their personal information to fraudsters. This often started by replying to an e-mail (e.g., clicking on a hyperlink) or by filling out information on a phishing website. In some cases, a perpetrator called end users and asked them to disclose personal information, including online banking credentials. In case of malware victimization, the devices used for online banking were infected with malicious software that was used to manipulate online banking sessions. How the infections took place was unclear from the case analyses study, because there was no detailed information on this in the bank's incident database. However, the interview study revealed that most victims' devices were automatically infected when surfing to websites with outdated security. Finally, the perpetrator monetized the stolen information. These steps are similar to what is known from the literature (e.g., Hong, 2012).

The answer on the 'why-question' is similar for phishing and malware attacks on online banking. End users complied with the malicious instructions they saw on their screens or that were instigated by the perpetrator. Cooperation was achieved because the social or technical engineering techniques used were successful, for instance, because the messages were perceived to be professional and trustworthy. Such messages typically respond to actuality, convey a sense of urgency and appeal to trust and authority. These factors are similar to what is found in the literature (e.g., Vishwanath, Herath, Chen, Wang, & Rao, 2011). Furthermore, end users seemed insufficiently suspicious about what was going on. Even though end users did not always trust the intentions of the perpetrator, they were mentally unable to stop the fraudulent process. Underlying reasons for cooperating with the perpetrator include, not being aware of how fraudulent schemes manifest in practice, not being alert at the right moment and having insufficient knowledge of online banking procedures and precautionary measures.

Besides providing insight into how and why end users became victims of online banking fraud – through their understanding of the situation (cognitions) and behaviour – it was interesting to investigate whether evidence could be found for certain characteristics of victims making them more prone to fall for such attacks. Because previous quantitative cybercrime studies failed to agree on universal characteristics, this thesis adopted a qualitative approach. Hence, the following sub-question was formulated: *2b) What end-user characteristics can be identified that increase the chance of online banking fraud victimization?*

The suitability factors from the routine activity approach that were tested – value, visibility and accessibility – did not seem to affect online banking fraud victimization. In addition, victims were distributed across genders, age categories and levels of education. The conclusion, based on the current findings, is that everyone is susceptible to phishing and malware attacks to some extent. In other words, no specific characteristics of end users could be identified that increase the chance of online banking fraud victimization.

The impact of online banking fraud victimization was included in the third sub-question: *2c) What are the effects and impact of online banking fraud victimization?* The interview study highlighted that besides (initial) financial effects (most victims tended to be reimbursed), there were also other different types of psychological and emotional effects. Examples include feeling awful, stupid and stressed and losing trust in banks and/or online banking, people in general and in themselves. The effects were mostly present during the first moments after victims became aware of what had happened to them. However, some of these effects were also evident in the long term. Furthermore, secondary effects were felt that were either instigated by the contact victims had with their bank or with the police in reporting and handling the incident, for instance time loss and having no direct access to money because the person's bank account was blocked. Nonetheless, some of the victims were satisfied with the ways the banks and the police handled their case. Concerning the impact of incidents, responses ranged from no or little impact to severe impact.

The fourth sub-question was formulated as follows: *2d) How do victims cope with online banking fraud victimization?* Victims had various cognitive and behavioural coping strategies to deal with their victimization. Cognitive strategies mainly concerned with reducing psychological and emotional distress and increasing online resilience regarding future attacks, i.e., having learned from the experience. The main behavioural strategies that were identified were reporting the incident to the bank and the police and seeking support from the social environment. This is, however, logical because the victims were identified based on police reports. In addition, various actions were taken regarding

installing new or additional technical protective measures on devices, being more alert or aware of fraudulent schemes, being more careful or precise when using online banking, making changes with regard to bank accounts and becoming more suspicious of e-mails. However, it was observed that some of these actions were only of limited duration. Some also adopted avoidance behaviours, for instance, using online banking services less. Victims who suffered financial damage as a result rationalized the incident, thereby minimizing victimization for themselves.

10.4 How can precautionary online behaviour of end users be explained and improved?

The third and final research question is answered based on evidence collected from Chapters 6 to 9. These chapters include the survey based on a sample of 1,200 online banking users, the secondary analysis of survey data based on a sample of 1,622 self-employed entrepreneurs and the experimental study about fear appeals involving 786 internet users.

The first sub-question dealt with the theoretical foundation of Part II of this thesis: *3a) What theoretical models can explain precautionary online behaviour?* As shown in Chapter 6, several models may explain this type of behaviour. It was found, however, that protection motivation theory stood out, not only because of its predictive ability, but also because of its applicability for interventions. Nevertheless, the reasoned action approach was also useful for explaining precautionary online behavioural intentions. Hence, the integrated model explained most variance in protection motivation, i.e., behavioural intention.

The second sub-question that was addressed is the following: *3b) What are the predictors of precautionary online behaviour?* The most important predictors are response efficacy, i.e., perceptions of how effective a protective measure is in reducing or mitigating a threat, and self-efficacy, i.e., perceptions of one's ability in carrying out the protective measure. This finding is similar to the studies on private and corporate end users that are described in this thesis. This is also consistent with results found in previous studies of the information security domain (Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015; Crossler, 2010; Ifinedo, 2012; Lee, 2011; Liang & Xue, 2010; Workman, Bommer, & Straub, 2008) and beyond this domain (Floyd, Prentice-Dunn, & Rogers, 2000; Milne, Sheeran, & Orbell, 2000). Attitude towards performing precautionary online behaviour was also found to be an important predictor. Secondary determinants were perceived severity, i.e., the perceived impact of a threat occurring, and internal locus of control, i.e., the extent to which an end user believes that he or she is mainly responsible for preventing an attack from being successful.

The third sub-question was formulated as follows: *3c) To what extent do the predictors of precautionary online behaviour differ between subgroups (gender, age, and education level)?* For private end users, there were significant differences between women and men. First, women's protection motivation was more influenced by the extent they believe that other people take precautions against security threats posed by online banking than is true for men. Second, with increasing age, women's protection motivation is stronger, but this was not true for men. Apart from this gender-related age difference, no significant differences were directly observed for age per se. Regarding education level, two differences could be identified regarding precautionary behaviour. First, the protection motivation of those without higher levels of education was more influenced by the extent they believe that other people take precautions against security threats posed by online banking than those with higher levels of education. Second, the protection motivation was more strongly negatively influenced for those with higher levels education by the extent to which they trust online banking (by reducing the perception of risk, which then decreased protection motivation), as opposed to those without higher levels of education.

For corporate end users, differences in precautionary behaviour were related to age and education level. The results indicate that older self-employed entrepreneurs take measures to protect their IT systems and data to a greater extent than their younger counterparts do. Furthermore, the results show that precautionary behaviour decreases as the level of education increases.

After having studied a range of aspects in order to 'understand' the phenomena at hand, effort was made to 'improve' the online resilience of end users. This was the central theme of the fourth sub-question: *3d) To what extent can predictors of precautionary online behaviour be influenced in order to improve end-user behaviour?* According to Wijn, Van den Berg, Wetzer, and Broekman (2016) two strategies can be used to influence user behaviour: increasing precautionary behaviour or decreasing risky behaviour. As opposed to previous studies that focussed on promoting precautionary behaviour (Chapters 6 to 8), the study presented in Chapter 9 examined whether internet users could be dissuaded from sharing personal information online through fear appeals so that susceptibility to phishing attacks could be reduced. This pre-test post-test study demonstrates that fear appeals have positive effects on heightening end-users' cognitions, attitudes and behavioural intentions. However, direct effects on subsequent security behaviour were not directly observed.

10.5 Theoretical and practical implications

In this section, the findings are discussed and the scientific and practical values are presented. This section includes implications for risk perceptions (10.5.1),

online banking fraud victimization (10.5.2), precautionary online behaviour (10.5.3) and general implications (10.5.4). The section then continues with an overview of the most important recommendations and provides an answer to the central question of this thesis (10.5.5).

10.5.1 Risk perception

More insight was gained in risk perceptions and predictors for risk perception in the online domain, specifically into the safety and security of online banking. End users perceive the potential impact of online banking fraud to be severe, but the chances of being victimized themselves to be slim. This is not a strange conclusion, because most online banking transactions do not go amiss. Furthermore, end users have relatively good levels of trust in online banking. From a bank's perspective this is promising, as it will not stop people from using online banking services. However, there is a potential downside to it.

The literature has shown a correlation between risk perception and communicating the advantages of (high-risk) activities (Finucane, Alhakami, Slovic, & Johnson, 2000). The greater the level of trust or the advantage of a certain activity, the lower the perception of risk and vice versa. Therefore, it is important for banks to find the right balance between the convenience and the security of their services.[52] This applies not only to using online banking services, but also to communicating about these services.

Indeed, underestimating risks can encourage people to behave unsafely, which ultimately increases risk (Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011). Hale (1996), for example, argues that having some degree of concern when it comes to crime is a good thing, so that people guard against it. However, overestimating risk can also have negative consequences, such as avoiding behaviour, e.g., not using online banking services as much. Thus, although increased awareness of fraudulent schemes should reinforce the ability of both private and corporate customers to recognize fraudulent schemes and act accordingly, it must not lead to customers becoming unhappy and distrustful. A quote from Frank Crane sums this up really well: 'You may be deceived if you trust too much, but you will live in torment if you don't trust enough'. The bottom line is that customers should only engage in online banking practices if things go exactly as planned and expected. When communicating about risk, the results of this research reveal that the most important predictor to consider is perceived vulnerability, which appeals to personal relevance. However, as we

[52] This balance or trade-off between convenience (easy access to your money) and security (wanting your money to be absolutely safe and secure) is basically the essence of cybersecurity in online banking.

will see later, it is important to also include information on coping measures against threats in that particular communication.

Furthermore, end users perceive the chance that others will fall victim to online banking fraud to be higher than their own chances. This can be justified by the following (Bragdon, 2008). People operate on the basis of assumptions and personal beliefs that enable them to set goals, plan activities, and so on. Over time, this 'conceptual system' evolves and offers them expectations about their surroundings. People act based on this conceptual system of assumptions without having any evidence for it. One of these assumptions is the belief in personal invulnerability. For example, people acknowledge that crimes occur a lot, but at the same time, they believe that it will not happen to them. They underestimate their own risks and overestimate others' (Workman et al., 2008). Generally speaking, people are not very good at assessing risk (West, 2008).

Trust is an important aspect in online banking. In this thesis, trust is studied on a general level – as a (moderate) predictor of perceived risk. Future studies could adopt a more specific focus on trust in online banking. Knowing how online trust develops and how an optimal level of trust can be maintained is a necessary requirement when organisations, such as banks, become more dependent on online service delivery (Beldad, De Jong, & Steehouder, 2010). Furthermore, although more is known about trust in online banking in general, it would be interesting for future research to study how trust applies to different online payment products, such as iDeal, PayPal, AfterPay and credit cards. Which would banking customers choose, in which cases and why? And perhaps with regard to crypto currencies too, which are becoming increasingly popular.[53]

An aspect that was lacking in the literature on what constitutes perceived risk in the online context was victimization. In this thesis, three types of victimization were included to examine whether they affected risk perception. However, these variables proved to be of less value in explaining risk perception as opposed to the more robust measures of perceived vulnerability, perceived severity and trust in online banking. Although 64% of the variance for risk perceptions of online banking fraud was explained, future studies are needed to further understand how risk perceptions are formed. Applying the psychometric paradigm to online risks (e.g., Garg & Camp, 2012; Van Schaik et al., 2017) and including additional characteristics of end users, such as personality traits (e.g.,

[53] Maartens, L. (2017). *De onweerstaanbare opkomst van Bitcoin* [The unstoppable rise of Bitcoin]. Retrieved from https://www.telegraaf.nl/nieuws/302759/de-onweerstaanbare-opkomst-van-bitcoin

Borwell, Jansen, & Stol, 2018; Halevi, Lewis, & Memon, 2013; Parsons, McCormac, Butavicius, & Ferguson, 2010) are options.

In conclusion, locus of control was added as a potential predictor variable of perceived threat. Although significant, the effects were minimal. It can be argued, also in relation to the studies described in Chapters 6 and 7, that locus of control is more concerned with assessing coping mechanisms than it is for threat assessment. Therefore, future studies should test perceived personal control (Griffin et al., 2004; Hajli & Lin, 2016) on risk perceptions as this more specific construct has better predictive ability for risk perceptions.

10.5.2 Online banking fraud victimization

More light has been shed on online banking fraud victimization. Real-world data, gathered from a bank's information system, and interview data were used to explain online banking fraud victimization. This section is divided into the following sub-sections: the victimization process, victim characteristics and coping with victimization.

The victimization process

It can be concluded that end users have an unintended and subconscious yet active role in their own victimization. This counts primarily for phishing victimization, but to a certain extent also for malware victimization. Although malware can be considered a type of technical engineering, end users still had to act for some of these attacks to be successful. Hence, both attack types are similar in many ways. Leukfeldt, Kleemans, and Stol (2017) also demonstrate that the goal of phishing and malware attacks (i.e., stealing money from online bank accounts) and the modus operandi of both attack types (i.e., intercepting login credentials, intercepting one time transaction authentication codes, wiring the money to money mule accounts and cashing the money) are quite similar. A difference between the two attack types is that phishing attacks often involve direct contact between the victim and the perpetrator, while the contact for malware attacks was indirect, i.e., mediated by technology.

The importance of trust is not limited to risk perceptions, but includes also actions of online banking users. Sometimes trust stops people from adequately countering phishing or malware attacks. As Luo, Zhang, Burd, and Seazzu (2012) argue, phishing attacks often succeed because cognitive biases in human thinking are exploited, rather than because the perpetrators take advantage of technological loopholes. Phishing victimization is largely caused through heuristic processing. Victims trust the perpetrator when asked to perform actions with fraudulent outcomes over the phone, they trust the deceitful message that pops up their computer screen, and they trust the phishing e-mail they have received.

They were tricked into doing so using the psychology of persuasion, mainly because perpetrators appeal to trust and authority.[54] Recently, phishing messages have started to appear on mobile phones via SMS.[55]

A relevant question concerning e-mails is whether banks should continue to use e-mails – to private e-mail accounts – as a communications channel. The disadvantage of banks sending e-mails to private addresses is that the phishing crime script often starts by sending an e-mail. This is even more the case since phishing e-mails are becoming increasingly professional, which means that they are more difficult to distinguish from legitimate ones. If banks were to stop sending e-mails to private (or business) addresses, and limit sending e-mails to the secure online banking environment of their customers, then customers would not have to decide whether the e-mail was legitimate or not. However, commercial reasons will probably preclude such a measure from being taken. Yet, from a customer perspective, this could reduce the risk of falling for phishing scams.

In addition, some victims mentioned that during the attack their gut feeling told them that something was wrong. However, they were mentally unable to stop the fraudulent process. Somehow, end users do not dare to explicitly doubt that it is the bank that is on the phone. Alternatively, they were simply not paying enough attention at that particular moment. Future research should identify which signals in particular trigger this unsafe feeling and how that feeling can be empowered so people will act upon to it, i.e., start trusting their instincts. It is the same as driving a car; if in doubt, do not overtake.

It is also advisable to inform users – at least in general – how perpetrators operate in fraudulent schemes, for example, what security codes entail, what happens when they fall into the wrong hands and which trust indicators perpetrators use in their advantage. The data showed that some victims were unfamiliar with the modus operandi (and influencing techniques) used in online banking fraud schemes or tended to have a lack of knowledge about information security practices. This is not remarkable, since information security is an abstract concept for many.

While the costs of implementing security measures are real and direct, they often have – in the case of online security – no visible outcome and the threats

[54] Clicking on a hyperlink in a phishing e-mail can be the result of habits, such as the habit of being deferential to people in authority (Bullée, 2017).
[55] ING (n.d.). *Phishing via SMS*. Retrieved from https://www.ing.nl/de-ing/veilig-bankieren/belangrijke-mededelingen/phishing-per-sms.html

they guard against are also often invisible (West, 2008). Therefore, explanations should be on a general level. To draw an analogy to driving a car again, people do not need to understand how everything works under the bonnet, but they have to know the basics so that they can avoid break downs.

An example of a general warning is: 'We never call you'. A crime script that was encountered often while working on this thesis clearly shows that criminals not only use fake e-mails and websites that appear to be sent by banks, they also call victims to intercept the necessary transaction codes. In this crime script, phone calls are a crucial part of the phishing attempt. The phishing e-mail and/or website may provide accesses to the victim's bank account, but perpetrators are still unable to transfer money. To actually transfer money, they require codes that have to be generated by the victim. Prevention campaigns should not only make customers aware of the fact that phishers are looking for these credentials, but also that they actually call people to get their hands on these codes. The campaign message can be simple and clear: 'no one ever asks for your transaction codes – not by phone either'.

A higher level of abstraction is also prudent when taking into account different online banking systems and procedures – used by different banks – and all of the other online threats end users are confronted with. It is not feasible to act against each specific threat if all are presented as being equally important. In addition, if they focus on one threat, people might become more vulnerable to another; it is impossible to warn online banking customers – or the broader internet population – about everything. It is even more complicated for corporate customers, as they have to be informed about new threats and coping measures, while not compromising on productivity.

Victim characteristics

Characteristics of end users that lead to higher chances of being victimized through online banking fraud could not be identified in this research. A qualitative approach using the routine activity approach was insufficient. Perhaps this is due to online activities not being distinctive anymore, because of their increased usage. Another option is that characteristics were not set-off against the non-victim population. Follow-up studies should also include a non-victim sample, so that comparisons between characteristics of victims and non-victims can be made. The lack of explanatory power of the routine activity approach could also be linked to the dragnet method that perpetrators usually use to target their victims. Leukfeldt (2015), who conducted a quantitative study using the same theoretical approach to study the same online threats, presented a similar explanation. It is possible that this conclusion only counts for online

banking fraud, and not for other types of cybercrime, such as CEO fraud, for which perpetrators have to delve into someone's background.

Online banking fraud victims are not selected because of their suitability factors or routine activities; instead attempts are made to reach them by sending out untargeted bulk e-mails in the hope that someone will bite. This is a cost-effective method for perpetrators, which pays-off even if a small percentage falls for it (Jones, Towse, & Race, 2015; Parrish Jr, Bailey, & Courtney, 2009). The contents of the attacks are continually adjusted to be in line with recent events and succeed in gaining the trust of end users. This thesis found no hard evidence that spear phishing – a more labour-intensive type of social engineering – is being applied in online banking attacks. This is an indication that target suitability is probably not that important to perpetrators when it comes to online banking, even though the perception is that this kind of phishing attack has a higher success rate (Bursztein et al., 2014).

Attacks on online banking using malware can be instigated using various methods. In the interview study, it became clear that victims' devices were automatically infected with malware when visiting a website with outdated security. However, malware infections can also be spread using social engineering tactics, for example, by convincing a user to open an infected attachment in a fraudulent e-mail. Concerning infected websites, it is important to consider the role of website owners or hosting companies in combatting malware attacks on online banking since customers themselves seem to be quite defenceless against such schemes. This conclusion is drawn because victims noticed nothing out of the ordinary and their security systems did not pick up anything malicious when conducting bank activities online. In such a case, end users can hardly be considered the weakest link.

Besides the routine activity approach, data were also available on victims' demographics. No differences in victims' demographic attributes were evident in the fraud cases studied at banks, in the interviews conducted with victims or in the survey presented in Chapter 2. In other words, victims were equally likely to be male or female, young or old and levels of education made no difference. This leads to the conclusion that the victim population is very diverse. This is contrary to previous studies that suggested that scam victims are more likely to be older (e.g., Grimes, Hough, & Signorella, 2007).

This finding suggests that potential victims of online banking fraud are difficult to identify because people are all equally likely to fall victim. It could be that victimization is not a coincidence and that victims do have unique characteristics or behaviour patterns or are exposed to certain circumstances. In that case,

other variables predicting victimization should be studied or other means of data collection should be used when applying the routine activity approach. It would be useful to analyse real-world data in terms of online behaviour, for instance based on log files or information from online databases in which victims' contact information is stored. Additionally, it would be interesting to find out if there are any differences between online banking fraud victims and victims of phishing and malware attacks within other contexts.

An important implication, at least as it stands now, is that it may be potentially more worthwhile to carry on investing in prevention for the whole online banking population rather than for specific groups of customers, as it is not yet clear if there are subpopulations that run greater risks of being targeted. Indeed, victims are a heterogeneous target group. Alternatively, it may be more effective to disrupt the crime scripts that perpetrators use (Leukfeldt, 2016). Perhaps a two-pronged approach targeting user behaviour and perpetrator methods would be most effective in reducing online banking fraud victimization.

In line with the reasoning above, mainly based on observations beyond the context of the individual studies, banks should continue to invest in their own detection systems in order to stop fraudulent attacks from succeeding. Banks continually develop their detection systems, but it is essential to emphasize the importance of this here, especially because it is not clear how some of the malware attacks described in this thesis took place. Another recommendation that banks might consider is to build in a delay in money transfers, for example, if money is transferred to bank accounts used for the first time. The delay could for instance be 48 hours. Then both banks and customers have potentially more time to reveal fraudulent transaction attempts. By doing so, transactions can be declined so that virtually no damage occurs, benefiting both parties. Another option would be to process transfers during office hours only so that departments responsible for monitoring and detection can effectively anticipate fraud attempts. However, this is at odds with the speed that the economy demands, i.e., real-time transactions. Again, the incontrovertible fact is that not all fraudulent transactions can be stopped.

Coping with victimization

The conclusion that the target group of victims is heterogeneous also has implications concerning how to help victims recover from their victimization. This thesis has shown that victims deal differently with their victimization. The study on the effects and impact of online banking fraud revealed that the monetary aspect is not the only important one. For some, the incident had far-reaching psychological and emotional consequences that must not be ignored. This means that the actors involved, such as banks and law enforcement agencies, need to

understand that each individual victim has a range of needs that have to be attended to (Cross, Richards, & Smith, 2016) and they must respond adequately to those needs. When victims report incidents, an important starting point is that their victimization is recognized and that they are treated sensitively. The Dutch Ministry of Safety and Justice (2013) acknowledges this in their vision document on doing justice to victims. Not only is this important for the victim's recovery, it is also desirable from an ethical perspective.

An important finding is the value of discussing incidents with others, especially the social environment. This is important for coping with online banking fraud incidents. There still seems to be a stigma surrounding (online) fraud victimization, as victims themselves are sometimes seen as (partly) responsible for their victimization (Button, Lewis, & Tapley, 2009a; Cross et al., 2016). To remove that stigma, it is important that victims are reassured that they need not be embarrassed and that they are encouraged to talk more openly about it.[56] This may also benefit the willingness of victims to report such incidents to the police (Cross et al., 2016).

An observation that is interesting for banks as well as the police is providing feedback to victims on how the victimization took place. The assumption is that victims are then better able to learn from the actions that lead to victimization. This is especially the case for aspects that concern security, because unwise actions do not always translate directly into obvious negative outcomes, and that makes learning more difficult (West, 2008). Giving feedback about how the case is handled is also advisable, because it may help to restore a victim's trust.

Providing insight into the factors underlying victim responses to phishing and malware incidents was beyond the scope of this research, but it could be interesting for follow-up studies. Personal and situational factors affect appraisal processes. Personal factors include commitments and beliefs, in particular beliefs about personal control and existential beliefs. Situational factors involve novelty, predictability and event uncertainty, but also temporal factors including imminence, duration and temporal uncertainty and, ambiguity and the timing of a stressful event in the person's life course (Lazarus & Folkman, 1984). For secondary appraisal in particular, the resources that are readily available to individuals also play an important role. Examples of these include knowledge, money, tools, people to help and skills (Lazarus & Folkman, 1984). Insight into

[56] Turrill, K. (2017). *Have YOU been a victim of fraud? A third of UK adults have fallen for a scam TWICE*. Retrieved from https://www.express.co.uk/life-style/life/870986/action-fraud-benefit-uk-email-online-barclays

these phenomena would benefit our understanding of the victims' coping processes and the differences between them.

10.5.3 Precautionary online behaviour

More insight has been gained into precautionary online behaviour. Survey data gathered from online banking users, self-employed entrepreneurs and general internet users were used to explain this type of behaviour. This section is divided into the following sub-sections: theoretical basis for studying precautionary behaviour, predictors of precautionary behaviour and behavioural change.

Theoretical basis for studying precautionary behaviour

The way end users make decisions related to information security is what Parsons et al. (2010) call a dynamic and complex matter. Decisions are, for example, influenced by end-users' cognitive abilities and biases in their thinking. End users also have different learning strategies and there are various strategies for protecting end users against online threats. Alsharnouby, Alaca, and Chiasson (2015) describe four complementary strategies to protect end users against phishing: (1) automated phishing detection; (2) manual phishing detection (user interface cues); (3) education on precautionary behaviour; and (4) designing protection mechanisms by understanding end-user's susceptibility to phishing.

This thesis tested which theoretical model best explains precautionary online behaviour in the case of online banking. The protection motivation theory (PMT) and the reasoned action approach (RAA) both explain a significant amount of variance for behavioural intention. Moreover, the integrated model explained the highest levels of variance, giving practitioners potentially more options when it comes to prevention campaigns, because the variables that were significant predictors in the individual models remained significant when studied in combination. This conclusion is consistent with the work of Herath and Rao (2009) and Ifinedo (2012).

In line with previous studies that have adopted PMT as their theoretical framework, the studies in Chapters 6 to 8 adopted PMT as a theory of behaviour, even though it can be argued that PMT is a theory of behavioural change rather than a theory of behaviour (Johnston, Warkentin, & Siponen, 2015). However, this thesis demonstrates that PMT is useful as a theory of behaviour as well, one which can be used to understand which drivers for precautionary behaviour are most important for specific contexts. Hence, the results from Chapters 6 to 8 provided additional grounds for the manipulation of particular variables in the fear appeals study in Chapter 9.

Predictors of precautionary behaviour

More insight was gained into what motivates end users to take precautionary measures for safe and secure online banking, and into what motivates self-employed entrepreneurs to take technical and personal precautionary measures. The studies in this thesis showed that, for private and corporate end users alike, response efficacy and self-efficacy were the most important predictors for precautionary online behaviour. This finding has implications for security education, training and awareness (SETA) campaigns. Hence, the focus of such campaigns should theoretically be on these aspects, for instance, promoting the effectiveness and ease of use of a measure in mitigating a certain treat; what is the right behaviour and what does it aim to solve or prevent. That measures should be easy to use is also demonstrated by the fact that security is perceived to be a secondary task by most end users (Alsharnouby et al., 2015).

Threat variables did not seem to explain much of the variance in the models. There is a theoretical explanation for why threat variables do not seem to be strong predictors of protection motivation. Milne et al. (2000) indicate that the weaker association of threat variables with protection motivation may be due to statistical interpretations and operationalization. This is because risk may have a positive and a negative relationship with behaviour. There is a positive relationship when someone feels vulnerable to a certain risk and therefore adopts precautionary behaviour. If precautionary behaviour has already been adopted, an individual may no longer feel vulnerable and therefore the relationship is negative. Longitudinal research might provide an explanation for how this relationship works. Nonetheless, besides explaining the effectiveness and usability of a particular coping measure, focus should also be on threat awareness, as it is believed that threat appraisal initiates the coping appraisal process. Adams and Sasse (1999) showed some 20 years ago that people are motivated to take precautionary measures as long as they are perceived to be necessary, for instance, because there is a clear external threat or the information is sensitive and needs to be safeguarded. The heart of the matter is that instead of trying to remove the risk, people should be made aware of how to manage the risk.

Furthermore, the studies described in Part II of this thesis showed that response costs should be kept low, in terms of money as well as time. Thus, an optimal balance must be found and maintained between usability and security. One way to characterize how users value information security is to quantify how they

make trade-offs related to cybersecurity.[57] For instance, how much loss of legitimate online content are users willing to incur to reduce the likelihood of a successful phishing attack? Or how much inconvenience are users willing to tolerate to reduce the chance of a phishing attack? These are interesting leads for further study.

In addition, end users should be made aware that they have a personal responsibility in keeping their online banking sessions safe and secure, so an appeal should be made to their internal locus of control. In addition, customers should also realize that security is never completed; it is an ongoing fact of life. If money is up for grabs, perpetrators will be looking to get their hands on it. Perpetrators will therefore continuously come up with new ways to crack the weakest link. In summary, customers should be made aware of what may happen, but also of what they can do to protect themselves. Moreover, safety and security requires the joint effort of banks and customers alike. This means that customers should be treated as peers in this endeavour. This also implies that banks should communicate about what they are doing to play their part for online banking safety and security.

This thesis provided insight in the drivers of precautionary behaviour and how these insights can be applied in practice. However, in order to better understand the drivers, it is fruitful to qualitatively explore how these drivers are formed in people's minds; Fishbein and Ajzen (2010) refer to these as beliefs. This is important, because a deeper understanding of beliefs might provide insight into how to influence the drivers more effectively and – indirectly – the target behaviour and its intentions. Priority could be given to investigating the beliefs that constitute response efficiency and self-efficacy, because these are the strongest predictors. Following this line of reasoning, an interesting possibility for future research would be to study mental models of customers concerning online banking fraud risks and how these relate to taking precautionary measures. This could improve our understanding of customer knowledge, attitudes and behaviours, and, possibly, how to influence these. Hence, it might help to explain the as-yet unaccounted for variance of the models in this thesis. Qualitative approaches are useful because there is a tendency to analyse behaviour on a population basis even though users are different, i.e., they do not all act in the same way.

Although the inclusion of a study on corporate end users in this thesis – in this case self-employed entrepreneurs – may be considered a unique component in

[57] Schneier, B. (2008). *The psychology of security (Part I).* Retrieved from https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html

information security research, more research into this target group as well as into small- and medium-sized enterprises and larger organizations, such as municipalities and hospitals, is required. In the media, stories are circulating about data being inadequately protected or even worse, being accessed (e.g., via discarded computers) or stolen using digital or online means.[58,59] In addition, corporate target groups have their own unique problems, such as CEO fraud and invoice scams. Precautionary online behaviour should extend across all layers of society and thus more research should be conducted into these target groups as well.

Behavioural change

When all is said and done, people's protection motivation or behavioural intention is just the starting point (Milne, Orbell, & Sheeran, 2002), because motivations have to be followed up by real actions. In order to understand whether theoretical recommendations work in practice, an experimental study on fear appeals was conducted. Fear appeals are a type of intervention that is receiving increasing attention in behavioural information security research (Wall & Buche, 2017). Protection motivation theory was chosen as the primary model. Variables concerning attitude and message rejection, i.e., resistance and two avoidance constructs, were included. These constructs are adopted from the extended parallel process model (Witte, 1992) and the stage model of processing of fear-arousing communications (De Hoog, Stroebe, & De Wit, 2005).

The study described in Chapter 9 demonstrates that fear appeals have positive effects on heightening end-users' cognitions, attitudes and intentions. However, effects on subsequent security behaviour were not directly observed. Thus, fear appeals have great potential to promote security behaviour by making end users aware of threats and simultaneously providing behavioural advice on how to mitigate these threats, but future research is needed to test how this can successfully transfer to the right behaviour, which is a crucial aspect in information security. Other research also demonstrates that fear appeals can be effective in promoting precautionary behaviour, although some inconsistencies remain which need to be resolved by future research (Wall & Buche, 2017). In

[58] Voort, S. van (2017). *Ziekenhuis meldt datalek na diefstal van laptop met patiëntgegevens* [Hospital reports data leak after laptop theft with patient data]. Retrieved from https://tweakers.net/nieuws/120469/ziekenhuis-meldt-datalek-na-diefstal-van-laptop-met-patientgegevens.html

[59] Nu.nl (2016). *Privédata duizenden inwoners Rotterdam en Oegstgeest gelekt* [Private data leaked of thousands of Rotterdam and Oegstgeest residents]. Retrieved from https://www.nu.nl/internet/4227550/privedata-duizenden-inwoners-rotterdam-en-oegstgeest-gelekt.html

order to understand why intentions are or are not followed by actions it is worthwhile investigating factors in this relationship, such as actual skills or abilities and environmental factors (Fishbein & Ajzen, 2010). In addition, the situational context, for instance, controlling for the mood of end users, e.g., being in a hurry, feeling tired and having experienced a traumatic life-event, is also an interesting lead for follow-up studies.

Although the intervention was set up realistically, it was still part of a study and participants were aware of this. The extent to which the results apply to real practice – making end users resilient when it comes to cyberattacks – needs to be more thoroughly examined in follow-up research. Myers and Abraham (2005) wrote a paper about the extent to which people adhere to advice given by healthcare professionals. They state (p. 680) that 'anything from 15 per cent to 93 per cent' of patients do not act on various recommendations and about 50 per cent do not take prescribed treatments, and this applies to both minor and major health conditions. Reasons for non-adherence include not remembering to take the treatment, not understanding it, not knowing how to follow it, but also disagreeing with diagnoses or medication regimen. They conclude that, although healthcare professionals have the right expertise, make accurate diagnoses and provide effective treatments, a substantial part of medical consultations has little or no impact on patients' health. If people do not care about their own personal health, or are not able to invest in it, what are they willing and able to do about their online safety and safeguarding it?

In conclusion, the results presented in this thesis are applied to the Dutch online banking context, but seem relevant to other contexts as well. For instance, they may be relevant when new security measures are implemented. Cross-sectional research is required to strengthen the applicability of the presented models and to test the results for robustness. Although cross-sectional research cannot provide definitive answers about causality, it does provide evidence that corresponds to causal hypotheses, for instance to those that are formulated in this thesis. However, finding true evidence for cause-and-effect-sequences calls for longitudinal research approaches. In addition, perceptions are not constant. The studies presented in this thesis provide a snapshot of perceptions at a particular point in time; that said, this is a common problem in social scientific studies. Therefore, it is advisable to repeat such studies in a few years' time.

10.5.4 General implications

The studies also have some implications at a higher level of abstraction; these are presented in this section. This section is divided into the following sub-sections: online banking system, online safety communications and final consideration.

Online banking system

Despite all the measures that one might take, there will always be a risk of losing money. The way in which online banking is currently designed, takes on the risk that it can be interpreted in different ways by different people. As stated in Chapter 3, if a fraudulent attempt is in line with the image that a customer has of reality, the risk of becoming a victim increases. This reality concerns, for example, an understanding of the online banking system and its processes, but it is also about knowing how an attack works, seeing one's own vulnerability and seeing how this vulnerability can be reduced or mitigated. Of course, customers cannot be aware of everything, and even if they could it would be a burden because there is so much that they need to know already. However, basic principles such as banks never deal with security issues by e-mail or telephone, what security codes entail and what happens when they fall into the wrong hands, are still called for. This thesis observed that crime scripts often use the topic of improving online banking security. If customers are better informed about perpetrators using this excuse to get their hands on customers' credentials, perpetrators will no longer be able to appeal to customers' concerns about safety and security. A potential difficulty here is that banks sometimes do call customers if there is any suspicion of fraud related to a money transaction. Furthermore, it is also advisable to emphasize in prevention campaigns that customers must rely on their own intuition; if something does not seem right, it probably is not.

The challenge is to create a reality that cannot be manipulated when spinning a fraudulent story. This would allow customers to recognize an anomaly more quickly, making them more capable of preventing fraud. Nevertheless, running risks online is comparable to running risks in the offline world. However, in the real world, some personal risk mitigation measures can be taken, for example, deciding how much cash to carry around. This kind of measure could also be taken online; in fact it is already being applied to some extent, e.g., setting maximum transfer limits and blocking debit cards from being used outside Europe. A variation in limits and usage options makes it potentially more difficult for perpetrators to commit fraud on a large scale.

Still, banks could go a step further, for example, by letting customers block functionality in their online banking that they are not using and by letting them increase the levels of technical security. This may give customers the feeling of being more in control of their online safety, and by doing so they can determine their own risk profile. Anecdotal evidence for this suggestion was gathered from interviews in which participants mentioned that they would be willing to make more effort so that they can have extra security. Moreover, such a solution

might be beneficial, since a one-size-fits-all solution probably does not exist. This suggestion could provide insight into what customers see as risks, as well as shedding light on where they experience obstacles in their online banking experience. End users, for example, disregard security practices in favour of convenience or because they think that harm will not befall them (Tam, Glassman, & Vandenwauver, 2010), but also do so to achieve other, more relevant objectives.

However, this solution will not suit everyone because the majority of customers will probably choose the path of least resistance when it comes to security efforts (West, 2008). A possible downside is that it will become too complex for end users; the more choices they have, the more difficult it is to understand their impact. As stated by Parsons et al. (2010, p. III) 'security functions need to be meaningful, easy to locate, visible and convenient to use'. As mentioned earlier, future research needs to find out where the boundary lies between what customers find acceptable – taking time, actions and options attributed to security in consideration – and the usability (or complexity) of online banking. This is because 'usable security' might be a part of the solution for improving the safety and security of online banking for end users (Kiljan, 2017).

In conclusion, it seems that fraud shifts when new technologies are introduced. For instance, whereas previously attacks targeted ATMs and the cloning of magnetic stripes on debit and credit cards, now the attacks on the banking systems focus on (or are committed via) online banking (apps).[60] If the presented recommendations – or new (technical) improvements – sort out into the proposed direction, and fraudulent attacks on online banking fraud consequently continue to decrease, the question then is where threats and perpetrators will shift towards. Will they move to other online services, diverge to other countries or will they use more physical types of attacks against (vulnerable) customers? This also implies a threat to risk interventions, because perpetrators will shift their focus. SIDN, the administrator of the .nl domain names, observed that organizations in the financial sector were less popular targets of criminal phishing campaigns in 2017. Instead, airline, construction and media companies were increasingly becoming the targets of phishing activities.[61]

[60] Nu.nl (2017). *Tieners opgepakt voor diefstal via Tikkie-phishingsite* [Teenagers arrested for theft via Tikkie-phishing website]. Retrieved from https://www.nu.nl/internet/4978703/tieners-opgepakt-diefstal-via-tikkie-phishingsite.html

[61] SIDN (2017). *Aantal phishingsites met Nederlandse topmerken ruim 40% toegenomen* [Number of phishing websites using top Dutch brands increased by more than 40%].

Online safety communications

An observation during the research project – not necessarily a finding from this research – was that the main communication concerning online banking safety and security is a one-size-fits-all message for the whole target group, covering all ages, education levels, preferences, and the like. The communication efforts of individual banks also seem to target their whole customer base, except of course those for special meetings for elderly customers and those organized at schools (e.g., seminars on preventing young people from becoming money mules). This implies – intuitively – that the current communication efforts are probably not effective per se, because specific target groups have different levels of risk perceptions (Tan & Sagala Aguilar, 2012), because individual needs are not accounted for (Parsons et al., 2010), and because the design and contents of a message might influence information processing (Petty & Cacioppo, 1986). Anecdotal evidence from the interview study showed that some victims indicated that awareness campaigns had not reached them, because they do not watch television, do not read newspapers or do not actively look online for such information on their own initiative. This is of course also applicable to education and training efforts.

Future research should therefore focus on the social psychology of communications between banks and their customers. Marketing research has shown that interventions are more effective if targeted or segmented approaches aimed at specific groups are used (French, 2011). It is important to understand the audience and their preferences, because messages may otherwise be ineffective. However, a meta-analysis on fear appeals – a specific type of intervention – conducted by Witte and Allen (2000) shows that, in general, individual differences do not appear to influence the processing of fear appeal messages. Therefore, it would be interesting to conduct studies on how effective security-related messages could be designed for the various target groups; via which channels they should be communicated and at what times; and what the value would be of such an approach compared to a one-size-fits-all approach.

Myers and Abraham (2005) provide some evidence of aspects in communications that might positively influence the intention to adhere to advice from healthcare professionals, which might be useful for practitioners when designing SETA campaigns. They state that written information increases adherence. Recall of oral information, on the other hand, is weak. Other aspects

---

Retrieved from https://www.sidn.nl/a/veilig-internet/aantal-phishingsites-met-nederlandse-topmerken-ruim-40-toegenomen-

that enhance recall of information and instructions, and subsequently adherence, are repetition, explaining beforehand what you are about to tell, stressing the importance and being specific. Personalisation of the information and presenting it positively also have an impact on adherence. Needless to say, communications must be presented in ways that customers understand.

Communicating about security can be difficult because security is an abstract concept for many. Since security is viewed as an abstract concept, perhaps it would be better to speak of safety when addressing end users. Security can be viewed as a topic that does not concern end users, but is instead an issue for others, such as service providers, software developers and computer scientist. Perhaps people can relate more to the concept of safety as something they can do something about rather than security. Follow-up research should investigate the extent to which this suggestion is actually meaningful. For banks, it would be important then to emphasize to their customers that safety is something that they can influence. This may present a challenge since customers in general expect online banking to be safe – and secure.

Final consideration

While this thesis obtained relevant information on how safety and security of online banking can be improved from an end-user perspective, it should be noted that end users, not only online but also in the offline world, are confronted with numerous potential threats. It is a fantasy to believe that people can protect themselves against all threats and be vigilant about all aspects of life 24/7. This would simply make living impossible. People have limited capacity for information processing and so they multitask routinely. As a result, few tasks or decisions are given full attention. Generally, people tend to make decisions based on learned rules and heuristics (Davinson & Sillence, 2010; West, 2008) and fraudsters take advantage of this. Although this decision-making method is not perfect, it is extremely efficient. Therefore, we have to accept that bad things will continue to happen online, but optimistically they can be kept to a minimum when the suggested recommendations are applied to practice.

10.5.5 Overview of recommendations

To conclude this section, that is to answer the central question of this thesis: *To what extent can the safety and security of online banking be improved from an end-user perspective?*, the most important recommendations are summed up below.

1. *Continue to invest in security education, training and awareness campaigns concerning threats aimed at online banking.*

Security training, training and awareness (SETA) are 'some of the most effective countermeasures against the human factor threats to information security' (Parsons et al., 2010, p. 31). The safety and security of end users can be improved by making them more aware of the threats in the first place, for instance, by making the issue personally relevant. This thesis found, amongst other things, that it is important to make it clear to customers how perpetrators work and which trust indicators they misuse. Because people face different kinds of threats every day and threats continue to evolve, it would be wise to focus primarily on general modus operandi. Another important aspect to focus on is the gut feeling of customers. Some customers got an uncomfortable feeling both during and shortly after the fraudulent activity, but still fell victim. This suggests that they acted against their own better judgment. Intervention programs could focus on encouraging customers to trusting their instinct when it comes to these kinds of scams.

Notably, awareness or threat perception needs to be accompanied by a coping strategy that is both effective and feasible for customers. Indeed, effort should not be invested in turning customers – who are often not specialists when it comes to security – into security experts. However, they should be educated so that they have the necessary skills and competencies (Parsons et al., 2010). According to them, education comprises the output from awareness and training and should ideally lead to end users making the right decisions or at least being aware of the consequences of threats and the consequences of their own (unsafe) behaviour. Thus, SETA programs should not only increase awareness, knowledge and the right attitude towards information security; they should ultimately be about acting correctly at the right time.

Moreover, it is important to test SETA campaigns on their effectiveness and apply those that work best (possibly in a segmented fashion), because it is not yet clear which interventions work best (for which target groups and for which threats). This thesis tested fear appeals in a phishing setting and found that this type of intervention has some potential to enhance internet users' precautionary behaviour, as it raised end-user cognitions, attitudes and behavioural intentions. However, a critical note needs to be made. This study showed that intentions or motivations for behaviour did not subsequently affect actual behaviour.

In addition, evidence was found that prior victimization increases motivation for precautionary behaviour, which makes a case for applying simulated attacks as a form of learning. Although experiential learning is important, i.e., end users will then be prompted to action, it should be noted that the learning effect, i.e., adopting certain kinds of precautionary online behaviour, might wane with time. This was reported in the interview study described in this thesis, but also in a

recent dissertation on social engineering. That dissertation found that a person who has been warned may be less prone to falling for scams, but that the effect is only temporal (Bullée, 2017). Therefore, future studies also need to take retention time into account, preferably over longer periods of time, e.g., more than six months as Purkait (2012) recommends.

A study by Alsharnouby et al. (2015) advocates that as much as possible should be automated or computerised to combat phishing attacks. Their argument is that improved browser security indicators and awareness campaigns resulted in only a 6% increase of phishing detection rates in comparison with Dhamija, Tygar, and Hearst's (2006) study nearly twenty years later. Moreover, they stress that alert and vigilant users are not better at reliably detecting phishing attack, which is contrary to Vishwanath et al.'s (2011) proposition. Although I agree that we should also invest in computerised techniques as a first line of defence, we still need SETA, because end users will continuously be confronted with phishing and other types of fraudulent cyberattacks that cannot be stopped by technical measures. Moreover, if SETA efforts should not focus on detecting fake e-mails and fake websites, it should at least focus on proper or precautionary online behaviour, for instance how individuals should handle their private information online.

2. *Focus on underlying cognitive dimensions in security education, training and awareness campaigns, most notably on response efficacy and self-efficacy.*

In this thesis, a case is made that good security is more about people – and what is in their heads – than about technology. Technology plays an important part in defending against threats, but when the attacks find loopholes in technology or work around it, people play the leading role. Therefore, in order to strengthen the role of customers in the safety and security of online banking, threat appraisals as well as coping appraisals should be improved. It is essential to adopt a value-based approach; customers should perform the right behaviour because they believe that it makes a difference (response efficacy). Furthermore, customers should be able to perform the right behaviour (self-efficacy). If these aspects are in place, then it is likely that end users will adopt precautionary behaviour and become a strong link in the information security chain, i.e., their online resilience will be enhanced. Additionally, information related to threat appraisal should be part of communications to customers as well, because it starts coping appraisal. This thesis provides evidence that perceived vulnerability is the most important predictor of threat appraisal – and that it appeals to personal relevance – but it needs to be handled carefully.

3. *Make clear that banks and customers are partners in keeping online banking safe and secure.*

The safety and security of online banking is not one party's responsibility, instead it is a joint responsibility of several parties, primarily banks and customers. This means that banks have to uphold their end of the bargain, keeping their systems safe and providing a secure internet connection between customer devices and their systems. In addition, there are some general recommendations that end users themselves should follow, such as the uniform safety rules for online banking[62] and (other) basic security hygiene rules[63]. These recommendations count for both private and corporate end users, although the impact within corporate settings may be higher if security is compromised, that is, the mistake of one employee can shut down the whole organizational network.

In the discussion about implementing these recommendations, one should not speak of compliance with such rules, but rather of adherence. As Myers and Abraham (2005) argue, adherence suggests a collaborative involvement, in this case between banks and their customers. Compliance on the other hand implies that customers should do what they are told by banks. If customers fail to do so, it is their own responsibility. Angela Sasse stresses that security should be considered to be team sport.[64] Another way of viewing it is treating security as part of customer care. The question then is how banks can build a caring relationship with their customers. After all, customers falling for a fraudulent attack is inevitable and a fixed group of potential victims cannot easily be identified. As a starting point, however, banks will have to start from a

[62] The safety rules are: (1) keep your security codes secret; (2) make sure that your debit card is not used by others; (3) secure the devices you use for online banking properly; (4) check your bank account regularly; and (5) report incidents directly to your bank. Note that incidents should also be reported to the police. If more cases are collected, the chance increases that the police will tackle the issue.

[63] Although safety cues were evaluated as ineffective, other good practices might still relevant to lowering the chances of becoming an online banking fraud victim, such as (1) do not think that you are not an interesting target for perpetrators, instead be aware of the threats; (2) never respond to spam or e-mails from unfamiliar sources; (3) never open or execute attachments, unless you know precisely what is in them; (4) do not be tempted to respond to pop-up messages asking for personal information or wanting to install applications from untrustworthy sources; and (5) listen to your gut feeling: when the unexpected happens or is asked for, or something is too good to be true, stop using online banking and/or terminate the conversation. Note that these recommendations, although supported by the current research, are examples and do not pretend to be novel and/or comprehensive.

[64] Cyber Risk Summer School (personal communication, June 22, 2016).

cooperative perspective, rather than from the perspective of imposing what to do or not do.

Finally, end users may not always be at fault when falling victim to online banking fraud. In a number of malware attacks, customer devices were automatically infected when visiting websites that were somehow compromised. In such cases, it cannot be concluded that end users are the weakest link. Hence, customers can be told to take action to prevent malware infections, such as installing anti-malware software, but what if regular websites have infected ads on them? Although coping measures must be included in communications about risks, for malware too, it is not always easy to come up with effective solutions. Hence, the objective effectiveness of (single and combined) security measures is hard to determine, if at all feasible. Therefore, it is better to also involve other (responsible) parties, such as website owners and hosting companies. Thus, to improve the safety and security of end users, users themselves and banks are not the only important players; all parties that have a role in the online banking fraud process are involved.

4. *Facilitate victims in their recovery process, primarily by providing feedback.*

Because online banking customers are continually confronted with phishing and malware attacks and online banking fraud victimization cannot be completely prevented, it is important to invest in helping victims to recover from the harm that is done to them. This goes further than administrative procedures, such as restoring the bank account and reimbursing the amount that was stolen. It is important to provide victims with feedback on how the attack occurred and what made it succeed. This can make the incident a more meaningful learning experience and it strengthens the online resilience of the bank's customers, rendering repeated victimization less likely. This is a task for banks and the police, possibly in conjunction depending on the complexity of the attack. In addition, it is necessary to recognize their victimization, to treat them carefully and to provide feedback on the handling of the incident. Victim support the Netherlands, an organization that assists in the processing of victimization, may also play an important role in this regard.

5. *Continue with research on the human aspects of online banking safety and security.*

A challenge for adequate information security behaviour is how to educate and train end users properly. The theoretical principles that were developed need to be tested in order to find out what works. This thesis tested one way of doing this based on fear appeals. The question remains whether this is a good or effective approach or that other methods would be more effective, such as

embedded training and simulated social engineering and technical engineering attacks. The study on corporate customers found that, when people are confronted with an attack, they are more inclined to take action. This was also mentioned in the stories of some of the online banking fraud victims that were interviewed. However, this recommendation might be difficult to follow up because of the ethical and practical issues associated with such interventions.

It is also necessary to find out on what scale and frequency SETA initiatives should be rolled out and how they should be designed. Would a one-time course or a yearly exam suffice? Should awareness and knowledge be updated each month? Or should these initiatives be done on an ad-hoc basis when new threats emerge (real-time education)? It is important to ensure that customers are cautious and alert in their behaviour, and continue to be so, also with regard to new developments and types of attack on online banking.

An answer should be found to the question of who is responsible for making end users resilient online. Are the individual banks responsible? Should it be arranged centrally, for instance, by the Dutch Banking Association or the Dutch Payments Organization? Should government take on this role given that the threats discussed are beyond the scope of online banking? Or is it the remit of end users themselves, who are expected to be self-reliant in this day and age? Since online banking fraud is waning in the Netherlands according to the statistics[65], the question is to what extent banks will be prepared to extend their responsibility, especially taking into account the efforts that they have already made. Another important question is how these efforts in making end user online resilient should be organized. Currently, there are many (non-coherent) initiatives in this area. The question is whether this creates the desired effect? Perhaps it is more sensible and beneficial that one (or a few) key actor(s) take on a coordinating role in this.

Another fruitful area to explore when it comes to changing behaviour for the better might be the area of 'choice architecture', especially the concept of 'nudge'. This topic was only briefly touched upon in this thesis, but deserves a mention. Perhaps it is good to use nudges on bank cards (e.g., 'beware of scams, don't give me to strangers') or on authentication devices (e.g., 'don't disclose my codes over the phone'). Future research could explore this concept and complementary options from social marketing (see e.g., French [2011]).

[65] NVB (2017). *Fraude met internetbankieren gedaald. Totale fraude in het betalingsverkeer toegenomen* [Online banking fraud has dropped. Total fraud in the payment system increased]. Retrieved from https://www.nvb.nl/nieuws/2712/fraude-met-internetbankieren-gedaald-totale-fraude-in-het-betalingsverkeer-toegenomen.html

10.6 Limitations

This section mainly deals with the limitations of the studies presented in this thesis. Because all individual chapters described the limitations of the particular methodology applied, this section mainly covers overarching research limitations. In addition, research directions that were planned, but could not be followed through are discussed. Furthermore, possibilities for new research directions are proposed as options for dealing with these limitations and shortcomings.

An issue in this thesis regards the definition of phishing. In Chapters 3 and 4, a deviating definition of phishing is used: 'a scalable act of deception whereby impersonation is used to obtain information from a target' (Lastdrager, 2014, p. 8). The deviating part concerns the term 'scalable', which was problematic in some debates. This was particular the case, when the phishing modus operandi included phone calls, i.e., one-to-one communication. Therefore, the term 'scalable' was abandoned in the phishing definitions used in the other chapters.

In the Netherlands, mobile banking is on the increase. Mobile banking differs from online banking on 'fixed' devices in terms of (reduced) functionality. For instance transfer limits are lower and money can only be transferred to known accounts. Moreover, up until now, online banking fraud has not targeted mobile devices as much. Because there might be differences in users' perceptions regarding online banking on fixed devices versus mobile devices, it would be interesting to investigate whether differences are observed in risk perceptions and precautionary online behaviour. From the survey sample (N = 1,200) – see Chapters 2, 6 and 7 – only 34 participants could be considered mobile-only bankers, so the sample size was considered too small for comparison with participants exclusively using fixed devices for online banking (N = 659). A question relevant for future research is whether 'mobile users' and 'fixed users' differ in their perceptions of online threats, and their drivers for and the actual uptake of precautionary behaviour. Moreover, it would be interesting to control for the platform mobile users have adopted, especially for malware-related attacks. It may be that iOS-users have a different sense of security as they use a more closed platform as opposed to Android-users who use a more open platform. In addition, it is important to investigate whether new (types of) risks will be associated with the mobile platform, particularly because the expectation is that mobile devices will be used even more in the near future.

One of the research directions that could not be acted upon, concerns the victimization aspect. It would have been interesting to investigate the extent to which prior victimization has an influence on precautionary behaviour. However, the sample of victims in the data file (Chapters 6 and 7) was too small to carry

out additional analyses (N = 27). Nevertheless, the impact of this possible predictor was to some extent tested in Chapter 8. In that particular study, prior victimization significantly predicted motivations for taking technical coping measures.

Furthermore, it would have been interesting to study possible underlying causes for victimization based on the survey data, for example based on attitudes, behaviour or respondent characteristics. Moreover, besides the 2.3% that experienced online banking fraud victimization themselves, about 35% had been confronted with attempted phishing attacks on online banking and about 15% with attempted attacks using malware. An interesting direction for follow-up studies is what prevents people who are confronted with online threats from not becoming victims, and therefore more resilient to online banking threats.

A shortcoming considering the survey study, especially with regard to Chapter 7, is that the variable 'habit' could not be included in the analysis. This potential predictor correlated too strongly with self-efficacy and protection motivation. As a result, it could not be included in the analysis, because self-efficacy and protection motivation belong to PMT's core nomology. Future research should investigate the value of this variable in the context of precautionary behaviour on online banking. Evidence for the importance of this variable – at least in an organizational setting – is provided by studies of Vance, Siponen, and Pahnila (2012) and Vishwanath, Harrison, and Ng (2016). Frank Crane's quote is also pertinent here: 'Habits are safer than rules; you don't have to watch them. And you don't have to keep them either. They keep you.'

User perceptions of bank reimbursement policies or 'perceived financial compensation' when fraud occurs could not be tested either on protection motivation. The newly constructed scale was not reliable for further analysis. Although it may be interesting to include this variable in follow-up research, it must be noted that although reimbursement can restore most of the financial damages to customers in cases of fraud, they still experience hindrance. For example, the bank can block the bank account from being accessed online, which makes it more difficult for customers to access their money. Perhaps the experience that something went wrong does not compensate for the damage being compensated. Furthermore, customers lose time when communicating with the bank about the incident and the handling of it, and when visiting the police to report the incident. They may also suffer psychological and emotional damage because someone accessed their bank account. In this sense, customers are committed to keeping online banking as safe as possible and to taking measures even if they are reimbursed. The same applies to the concept of insurance. Even though one is insured for a whole range of possible incidents,

one tries to make sure that none of these incidents will happen. In spite of this, the hypothesis remains, partly considering the discussion about reimbursement practices and policies related to online banking fraud.

In addition, on the subject of improving the safety and security from an end-user perspective, future research should consider investigating customer perceptions of responsibilities. In the context of online banking, some authors argue that banks implement technical measures with the purpose of shifting the responsibility onto their customers (Murdoch, Drimer, Anderson, & Bond, 2010). This is also addressed by Davinson and Sillence (2014, p. 156): 'If the bank can show that a customer has been "grossly negligent" (a term the bank is free to define themselves) then the full liability shifts to the consumer'. This does not, however, change the risks of online banking, as the risks are still in the system. Besides a focus on threat perception and precautionary behaviour, new studies should therefore also consider the extent to which customers understand their own responsibility in relation to online banking (Davinson & Sillence, 2014), a topic that is only briefly examined in this thesis.

A challenge for researchers is to conduct research in cooperation with banks on bank systems. For the studies in this thesis, bank data could be accessed only once (see Chapter 3). Banks have a lot of data at their disposal to enable such analyses, especially in terms of background features and online banking behaviour. Perhaps it would be possible to compare customer behaviour before and after incidents, and whether they fall back into old patterns or habits after having adopted precautionary measures. The advantage of doing this kind of research at banks is that they are in a better position to identify victims or disadvantaged customers than is possible based on survey research. However, obtaining the right data might be quite laborious, because bank systems and how these systems are used are not always unambiguous. Academia might be able to help banks with getting more meaningful data out of their systems based on how this data is recorded.

Moreover, future cooperation with banks could also focus on how to implement measures that focus on the human aspects of cybersecurity. It is relatively easy to quantify the achievements of technical security measures. For example, it is possible to generate reports on how much traffic or attacks a firewall has blocked. For social interventions, it will be more difficult to build a (business) case. An important question to answer is how to measure the success of these 'soft' types of interventions.

Finally, from an outsider's perspective, a potential threat to the current research is that not all could be said and done, given the involvement of organizations

who funded the project and the context being investigated. However, formal agreements were reached in advance making it possible for the researchers who were involved in the research program to publish their findings. As a result, the research was able to adopt a critical and independent view on the matters discussed. This means that the views expressed in this thesis are not necessarily those of the project's funders.

10.7 Concluding remarks

This thesis investigated risk perceptions of and victimization involving online banking fraud. It also developed and tested a model of precautionary online behaviour, mainly guided by the protection motivation theory. In addition, it tried to improve precautionary online behaviour of internet users using fear appeals. The findings indicate, among other things, that it is important to focus on cognitive processes in order to adequately protect against online banking fraud. This means that it is essential to address the human aspects of online banking safety and security, especially when it involves attacks using social engineering, but to some extent also when it involves attacks using technical engineering. Consequently, solutions should be sought in what Bruce Schneier calls the 'people problem', and thus not in the 'math problem'.[66] Implications of the study results were discussed and opportunities for follow-up research presented.

Combatting online banking fraud and cybercrimes in general continues to be an arms race that probably will not be won by the good guys anytime soon. It is important to be aware of the fact that, even though people can be made more aware of and resilient to cyberattacks, there will always be people that fall for a scam or catch some malware; no amount of preventive techniques will be able to stop this entirely. It is not feasible to expect people to be alert at all times. For example, in the Netherlands, 1,300 online banking transfers went wrong each month in 2016, mainly because people were sloppy when checking bank account numbers.[67] Therefore, having one hundred per cent security would be a utopia. If we are able to accept this as a fact of life, it will make our lives more optimistic rather than pessimistic. And if something does go wrong, it does not necessarily mean that it was done on purpose or that someone is to blame for it.

[66] Schneier, B. (2000). *Semantic attacks: The third wave of network attacks*. Retrieved from https://www.schneier.com/crypto-gram/archives/2000/1015.html#1

[67] Scheres, P. (2017). *Slordig: Zo vaak gaat geld overmaken fout* [Sloppy: Money transfers go wrong this often]. Retrieved from https://www.rtlz.nl/finance/personal-finance/slordig-zo-vaak-gaat-geld-overmaken-fout

However, if end users are more vigilant about what they do online and are more aware of how others can abuse the advantages of the internet, the lives of perpetrators will be made more difficult. Or at least the impact caused by these attacks may be reduced. Therefore, security education, training and awareness remain an important priority, especially for combatting social risks. Hence, information security practices should become part of our general skill set as people. This is a necessary requirement, also in view of future developments regarding the 'Internet of Things' and the 'Internet of Everything'.

Furthermore, it is important to arrive at a situation that is fair to people, also for those who do not understand how technology and protective measures work and/or those who have not chosen to use them in the first place. Therefore, potential solutions might also be found in the area of usable security, especially for non-savvy internet users. If vital decisions can be made, or common errors can be prevented, through secure usability design and by default settings that have the user's interest at heart – thus not through human decisions – it would seem that fewer errors will be made, leading to less victimization. Moreover, probably fewer investments need to be done in educating and training end users.

In conclusion, fortunately most online banking practices and most online activities go right in most cases. The internet is flourishing, which is evident from the millions of interactions and transactions that simultaneously take place every day between citizens, businesses and governments (Wall, 2008). We need to make sure that this will continue in the future. An important requirement for a safer and more secure internet is that the human factor is given a central place. I believe that behavioural information security studies – in conjunction with other scientific fields – can make a great contribution to a safer and more secure internet for all.

References

Aaron, G. (2010). The state of phishing. *Computer Fraud & Security*, *2010*(6), 5–8.

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H. & Nunamaker Jr, J. F. (2010). Detecting fake websites: The contribution of statistical learning theory. *MIS Quarterly*, *34*(3), 435–461.

Abraham, C.S., Sheeran, P., Abrams, D. & Spears, R. (1994). Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of HIV infection. *Psychology & Health, 9*(4), 253–272.

Adams, A. & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Aldás-Manzano, J., Lassala-Navarré, C., Ruiz-Mafé, C. & Sanz-Blas, S. (2009). Key drivers of internet banking services use. *Online Information Review*, *33*(4), 672–695.

Alsharnouby, M., Alaca, F. & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69–82.

Anderson, C. L. & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643.

Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing, 25*(2), 160–171.

Anderson, R. (2007). Closing the phishing hole - Fraud, risk and nonbanks. In *Proceedings of the Payments System Research Conferences* (pp. 1–16).

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J., Levi, M., Savage, S. (2012). Measuring the cost of cybercrime. In *Proceedings of the 11th Workshop on the Economics of Information Security*. Retrieved from http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

APWG (2015). *Phishing activity trends report: 4th quarter 2014*. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf

Arachchilage, N. A. G. & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312.

Arachchilage, N. A. G., Love, S. & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185–197.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215.

Barroso, C., Carrión, G. C. & Roldán, J. L. (2010). Applying maximum likelihood and PLS on different sample sizes: Studies on SERVQUAL model and employee behavior model. In: V. Esposito Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.), *Handbook of partial least squares: Concepts, methods and application* (pp. 427–447). Berlin: Springer.

Beaudry, A. & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly*, *29*(3), 493–524.

Beck, U. (1992). *Risk society: Towards a new modernity*. SAGE Publications Ltd.

Beldad, A., De Jong, M. & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, *26*(5), 857–869.

Bhattacherjee, A. & Sanford, C. (2006). Influence processes for information technology acceptance: An elaboration likelihood model. *Management Information Systems Quarterly*, *30*(4), 805–825.

Blackwell, R. D., Miniard, P. W. & Engel, J. F. (2001). *Consumer behavior (ninth edition).* South-Western: Thomson Learning.

Blythe, J. M., Coventry, L. & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Proceedings of the 11th Symposium On Usable Privacy and Security* (pp. 103–122).

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S. & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, *10*(34), 1022–1035.

Borwell, J., Jansen, J. & Stol, W. (2018). Human factors leading to online fraud victimization: Literature review and exploring the role of personality traits. In J. McAlaney, L. A. Frumkin & V. Benson (Eds.), *Psychological and behavioral examinations in cyber security* (pp. 26–45). IGI Global.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D. & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*(4), 837–864.

Bossler, A. M. & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Bragdon, C. (2008). *Transportation security*. Burlington, MA: Butterworth-Heinemann.

Briggs, P., Jeske, D. & Coventry, L. (2016). Behavior change interventions for cybersecurity. In L. Little, E. Sillence & A. Joinson (Eds.), *Behavior change research and theory: Psychological and technological perspectives* (pp. 115–135). Amsterdam: Academic Press.

Bronfman, N. C., Cifuentes, L. A. & Gutiérrez, V. V. (2008). Participant-focused analysis: Explanatory power of the classic psychometric paradigm in risk perception. *Journal of Risk Research*, *11*(6), 735–753.

Brouwers, M. C. & Sorrentino, R. M. (1993). Uncertainty orientation and protection motivation theory: The role of individual differences in health compliance. *Journal of Personality and Social Psychology*, *65*(1), 102–112.

Brown, J. S., Collins, A. & Duguid, P. (1989). Situated cognition and the culture of learning. *Educational Researcher*, *18*(1), 32–42.

Brown, S. L. & Whiting, D. (2014). The ethics of distress: Toward a framework for determining the ethical acceptability of distressing health promotion advertising. *International Journal of Psychology*, *49*(2), 89–97.

Bullée, J.-W. (2017). *Experimental social engineering: Investigation and prevention*. Enschede: University of Twente (PhD thesis).

Bullée, J.-W., Montoya Morales, A., Junger, M. & Hartel, P. H. (2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. In *Proceedings of the Inaugural Singapore Cyber Security R&D Conference* (pp. 107–114).

Bursztein, E., Benko, B., Margolis, D., Pietraszek, T., Archer, A., Aquino, A., Pitsillidis, A. & Savage, S. (2014). Handcrafted fraud and extortion: Manual account hijacking in the wild. In *Proceedings of the 2014 Internet Measurement Conference* (pp. 347–358).

Butler, R. (2007). A framework of anti-phishing measures aimed at protecting the online consumer's identity. *The Electronic Library*, *25*(5), 517–533.

Button, M., Lewis, C. & Tapley, J. (2009a). *A better deal for fraud victims: Research into victims' needs and experiences.* London: National Fraud Authority.

Button, M., Lewis, C. & Tapley, J. (2009b). *Fraud typologies and the victims of fraud: Literature review.* London: National Fraud Authority.

Button, M., Lewis, C. & Tapley, J. (2014a). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54.

Button, M., Nicholls, C. M., Kerr, J. & Owen, R. (2014b). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391–408.

CBS (2014). *Achtergrondkenmerken en ontwikkelingen van zzp'ers in Nederland* [Background characteristics and developments of self-employed entrepreneurs in the Netherlands]. The Hague: Statistics Netherlands.

CBS (2015a). *Bevolking 15 tot 75 jaar-oud* [Population aged from 15 to 75 years]. Retrieved from www.cbs.nl/nl-nl/achtergrond/2015/20/bevolking-15-tot-75-jaar-oud

CBS (2015b). *Voorzichtig op internet door bezorgdheid over veiligheid* [Cautious on the internet because of safety concerns]. Retrieved from http://www.cbs.nl/nl-NL/menu/themas/vrije-tijd-cultuur/publicaties/artikelen/archief/2015/voorzichtig-op-internet-door-bezorgdheid-over-veiligheid-2015.htm

CBS (2016a). *ICT, kennis en economie 2016* [ICT, knowledge and economy 2016]. The Hague: Statistics Netherlands.

CBS (2016b). *Veiligheidsmonitor 2015* [Safety monitor 2015]. The Hague: Statistics Netherlands.

Chang, J. J. & Chong, M. D. (2010). Psychological influences in e-mail fraud. *Journal of Financial Crime*, *17*(3), 337–350.

Chellappa, R. K. & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358–368.

Chen, L.-C. & Bansal, G. (2010). An integrated model of individual web security behavior. In *Proceedings of the 16th Americas Conference on Information Systems* (pp. 485–492).

Chenoweth, T., Minch, R. & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. In *Proceedings of the 42nd Hawaii International Conference on System Sciences* (pp. 1–10).

Cheshire, C., Antin, J. & Churchill, E. (2010). Behaviors, adverse events, and dispositions: An empirical study of online discretion and information control. *Journal of the Association for Information Science & Technology*, *61*(7), 1487–1501.

Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 18*(1), 308–333

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719–731.

Claessens, J., Dem, V., De Cock, D., Preneel, B. & Vandewalle, J. (2002). On the security of today's online electronic banking systems. *Computers & Security*, *21*(3), 253–265.

Cohen, J. (1988). *Statistical power analysis for the behavioural sciences*. Mahwah, NJ: Lawrence Erlbaum.

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588–608.

Compeau, D. R. & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189–211.

Corbitt, B. J., Thanasankit, T. & Yi, H. (2003). Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications*, *2*(3), 203–215.

Coventry, L., Briggs, P., Jeske, D. & Moorsel, A. van (2014). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In A. Marcus (Ed.), *Design, user experience, and usability. Theories, methods, and tools for designing the user experience* (pp. 229–239). Cham: Springer.

CPB (2016). *Risicorapportage cyberveiligheid economie* [Risk report cybersecurity economy]. The Hague: CPB Netherlands Bureau for Economic Policy Analysis.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187–204.

Cross, C., Richards, K. & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, *518*, 1–14.

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. In *Proceedings of the 43rd Hawaii International Conference on System Sciences* (pp. 1–10).

Crossler, R. E. & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, *45*(4), 51–71.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101.

Cunningham, L. F., Gerlach, J. & Harper, M. D. (2005). Perceived risk and e-banking services: An analysis from the perspective of the consumer. *Journal of Financial Services Marketing*, *10*(2), 165–178.

Dang-Pham, D. & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security*, *48*, 281–297.

Das, E. H., De Wit, J. B. & Stroebe, W. (2003). Fear appeals motivate acceptance of action recommendations: Evidence for a positive bias in the processing of persuasive messages. *Personality and Social Psychology Bulletin*, *29*(5), 650–664.

Das, T. & Teng, B.-S. (2004). The risk-based view of trust: A conceptual framework. *Journal of Business and Psychology*, *19*(1), 85–116.

DataIM. (2008). *Omschrijving Surveyvalidator* [Description of the Survey Validator]. Amsterdam: DataIM.

Davinson, N. & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*(6), 1739–1747.

Davinson, N. & Sillence, E. (2014). Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies*, *72*(2), 154–168.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340.

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies*, *38*(3), 475–487.

Denkers, A. J. & Winkel, F. W. (1998). Crime victims' well-being and fear in a prospective and longitudinal study. *International Review of Victimology*, *5*(2), 141–162.

DeValve, E. Q. (2005). A qualitative exploration of the effects of crime victimization for victims of personal crime. *Applied Psychology in Criminal Justice*, *1*(2), 71–89.

Dhamija, R., Tygar, J. D. & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581–590).

Dignan, J. (2005). *Understanding victims and restorative justice*. Maidenhead: Open University Press.

Dijk, J. van (2012). *The network society (third edition).* London: SAGE Publications.

Dimopoulos, V., Furnell, S., Jennex, M. & Kritharas, I. (2004). Approaches to IT Security in Small and Medium Enterprises. In *proceedings of the 2nd Australian Information Security Management Conference* (pp. 73–82).

Dinev, T. & Hu, Q. (2005). The centrality of awareness in the formation of user behavioral intention toward preventive technologies in the context of voluntary use. In *Proceedings of the International Conference of Information Systems* (pp. 1–5).

DNB (2016). *Jaarverslag 2015* [Annual report 2015]. Amsterdam: De Nederlandsche Bank.

Domenie, M. M. L., Leukfeldt, E. R., Wilsem, J. A. van, Jansen, J. & Stol, W. Ph. (2013). *Victimization in a digitised society: A survey among members of the public concerning e-fraud, hacking and other high-volume crimes*. The Hague: Eleven International.

Downs, J. S., Holbrook, M. B. & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (pp. 79–90).

Downs, J. S., Holbrook, M. & Cranor, L. F. (2007). Behavioral response to phishing risk. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit* (pp. 37–44).

Dutch Ministry of Security and Justice (2011). *De nationale cyber security strategie (NCSS): Slagkracht door samenwerking* [The national cyber security strategy (NCSS): Strength through collaboration]. The Hague: Ministry of Security and Justice.

Dutch Ministry of Safety and Justice. (2013). *Recht doen aan slachtoffers: Visiedocument* [Doing justice to victims: Vision document]. The Hague: Ministry of Safety and Justice.

EC (2013). *Cybersecurity strategy of the European Union: An open, safe and secure cyberspace*. Brussels: European Commission.

Einspruch, E. L., Lynch, B., Aufderheide, T. P., Nichol, G. & Becker, L. (2007). Retention of CPR skills learned in a traditional AHA Heartsaver course versus 30-min video self-training: A controlled randomized study. *Resuscitation*, *74*(3), 476–486.

Eurostat (2016). *Individuals using the internet for internet banking.* Retrieved from http://ec.europa.eu/eurostat/tgm/refreshTableAction.do;?pcode=tin00099&language=en

Finucane, M. L., Alhakami, A., Slovic, P. & Johnson, S. M. (2000). The affect heuristic in judgments of risks and benefits. *Journal of Behavioral Decision Making*, *13*(1), 1–17.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*, *9*(2), 127–152.

Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. MA: Addison-Wesley.

Fishbein, M. & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. New York: Taylor & Francis.

Floyd, D. L., Prentice-Dunn, S. & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Fransen, M. L., Smit, E. G. & Verlegh, P. W. (2015). Strategies and motives for resistance to persuasion: An integrative framework. *Frontiers in Psychology*, *6*, 1–12.

French, J. (2011). Why nudging is not enough. *Journal of Social Marketing*, *1*(2), 154–162.

Frieze, I. H., Hymer, S. & Greenberg, M. S. (1987). Describing the crime victim: Psychological reactions to victimization. *Professional Psychology: Research and Practice*, *18*(4), 299–315.

Furnell, S. M. (2008a). It's a jungle out there: Predators, prey and protection in the online wilderness. *Computer Fraud & Security*, *2008*(10), 3–6.

Furnell, S. M. (2008b). End-user security culture: A lesson that will never be learnt? *Computer Fraud & Security*, *2008*(4), 6–9.

Furnell, S. M., Bryant, P. & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410–417.

Furnell, S. M. & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*, 983–988.

Furnell, S. M., Jusoh, A. & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27–35.

Furnell, S. M., Tsaganidi, V. & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security*, *27*(7), 235–240.

Gale, J.-A. & Coupe, T. (2005). The behavioural, emotional and psychological effects of street robbery on victims. *International Review of Victimology*, *12*(1), 1–22.

Garg, V. & Camp, J. (2012). End user perception of online risk under uncertainty. In *Proceedings of the 45th Hawaii International Conference on System Sciences* (pp. 3278–3287).

Garg, V., Huber, L., Camp, L. J. & Connelly, K. (2012). Risk communication design for older adults. *Gerontechnology*, *11*(2), 166–173.

Garland, D. (2003). The rise of risk. In R.V. Ericson & A. Doyle (Eds.), *Risk and morality* (pp. 48–86). University of Toronto Press.

Grabner-Kräuter, S. & Faullant, R. (2008). Consumer acceptance of internet banking: The influence of internet trust. *International Journal of Bank Marketing*, *26*(7), 483–504.

Green, D. L., Choi, J. J. & Kane, M. N. (2010). Coping strategies for victims of crime: Effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping. *Journal of Human Behavior in the Social Environment*, *20*(6), 732–743.

Griffin, R. J., Neuwirth, K., Dunwoody, S. & Giese, J. (2004). Information sufficiency and risk communication. *Media Psychology*, *6*(1), 23–61.

Grimes, G. A., Hough, M. G. & Signorella, M. L. (2007). Email end users and spam: Relations of gender and age group to attitudes and actions. *Computers in Human Behavior*, *23*(1), 318–332.

Gupta, A. & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, *13*(4), 297–310.

Gurung, A., Luo, X. & Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management & Computer Security*, *17*(3), 276–289.

Hair, J. F., Hult, G. T. M., Ringle, C. M. & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Los Angeles: SAGE Publications.

Hajli, N. & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, *133*(1), 111–123.

Hale, C. (1996). Fear of crime: A review of the literature. *International Review of Victimology*, *4*(2), 79–150.

Halevi, T., Lewis, J. & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd international conference on World Wide Web companion* (pp. 737–744).

Hanslmaier, M. (2013). Crime, fear and subjective well-being: How victimization and street crime affect fear and life satisfaction. *European Journal of Criminology*, *10*(5), 515–533.

Harrell, E. & Langton, L. (2013). *Victims of identity theft, 2012.* Washington DC: Bureau of Justice Statistics.

Harris, M. A. & Patten, K. P. (2014). Mobile device security considerations for small-and medium-sized enterprise business mobility. *Information Management & Computer Security*, *22*(1), 97–114.

Hayes, A. F. (2014). Introduction to mediation, moderation, and conditional process analysis: A regression-based approach. *New York: Guilford Publications*.

Hayes, A. F. (2016). *PROCESS (version 2.16).* Retrieved from www.processmacro.org

Hayes, A. F. & Preacher, K. J. (2014). Statistical mediation analysis with a multicategorical independent variable. *British Journal of Mathematical and Statistical Psychology*, *67*(3), 451–470.

Henseler, J., Ringle, C. M. & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In R. R. Sinkovics (Ed.), *Advances in International Marketing* (pp. 277–320). Bingley: Emerald.

Henson, B., Reyns, B. W. & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 475–497.

Herath, T. & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms* (pp. 133–144).

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81.

Hoog, N. de, Stroebe, W. & Wit, J. B. de (2005). The impact of fear appeals on processing and acceptance of action recommendations. *Personality and Social Psychology Bulletin*, *31*(1), 24–33.

Hoog, N. de, Stroebe, W. & Wit, J. B. de (2007). The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: A meta-analysis. *Review of General Psychology*, *11*(3), 258.

Huang, D.-L., Rau, P.-L. P. & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, *29*(3), 221–232.

Huang, D.-L., Rau, P.-L.P., Salvendy, G., Gao, F. & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870–883.

Hulland, J., Ryan, M. J. & Rayner, R. K. (2010). Modeling customer satisfaction: A comparative performance evaluation of covariance structure analysis versus partial least squares. In: V. Esposito Vinzi, W. W. Chin, J. Henseler, & H. Wang (Eds.), *Handbook of partial least squares: Concepts, methods and application* (pp. 307–325). Berlin: Springer.

Hulst, R. C. van der & Neve, R. J. M. (2008). *High tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie* [High tech crime, types of crimes and offenders: An inventory of literature.]*.* The Hague: Boom Juridische Uitgevers.

Hutchings, A. & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the net? *Current Issues in Criminal Justice*, *20*, 433–451.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79.

Jackson, J. (2009). A psychological perspective on vulnerability in the fear of crime. *Psychology, Crime & Law*, *15*(4), 365–390.

Jackson, J., Allum, N. & Gaskell, G. (2005). Perceptions of risk in cyber space. In R. Mansell & B. S. Collins (Eds.), *Trust and crime in information societies* (pp. 245–281). Northampton, MA: Edward Elgar.

Jakobsson, M. (2007). The human factor in phishing. *Privacy & Security of Consumer Information*, *7*, 1–19.

Jansen, J. (2015). Studying safe online banking behaviour: A protection motivation theory approach. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance* (pp. 120–130).

Jansen, J., Kop, N. & Stol, W. (2017). Internetbankieren: Veiligheidspercepties van gebruikers [End-user perceptions of safety and security of online banking]. *Tijdschrift voor Veiligheid, 16*(1), 36–51.

Jansen, J. & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In: *Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24–31).

Jansen, J. & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91.

Jansen, J. & Schaik, P. van (2016). Understanding precautionary online behavioural intentions: A comparison of three models. In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance* (pp. 1–11).

Jansen, J. & Schaik, P. van (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security*, *25*(2), 165–180.

Jansson, K. & Solms, R. von (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593.

Johnson, E. J. & Tversky, A. (1983). Affect, generalization, and the perception of risk. *Journal of Personality and Social Psychology*, *45*(1), 20–31.

Johnston, A. C. & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566.

Johnston, A. C., Warkentin, M. & Siponen, M. T. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*(1), 113–134.

Jones, H., Towse, J. & Race, N. (2015). Susceptibility to email fraud: A review of psychological perspectives, data-collection methods, and ethical considerations. *International Journal of Cyber Behavior, Psychology and Learning*, *5*(3), 13–29.

Kahneman, D. (2011). *Thinking, fast and slow*. London, UK: Penguin Group.

Kiljan, S. (2017). *Exploring, expanding and evaluating usable security in online banking*. Heerlen: Open University of the Netherlands (PhD thesis).

Kirlappos, I. & Sasse, M. A. (2012). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, *2*, 24–32.

Kloosterman, R. (2015). *Slachtofferschap cybercrime en internetgebruik* [Cybercrime victimization and internet use]. The Hague: Statistics Netherlands.

Koeske, G. F. & Koeske, R. (2006). A typology of outcome patterns in three-variable models: The pervasive role of mediation in causal systems. *Journal of Social Service Research*, *33*(1), 1–36.

Kok, G., Bartholomew, L. K., Parcel, G. S., Gottlieb, N. H. & Fernández, M. E. (2014). Finding theory- and evidence-based alternatives to fear appeals: Intervention mapping. *International Journal of Psychology*, *49*(2), 98–107.

Kritzinger, E. & Solms, S. H. von (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A. & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. In: *Proceedings of the 5th Symposium on Usable Privacy and Security* (pp. 1–12).

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*(2), 7:1–7:31.

Kunst, M. J. J. & Dijk, J. J. M. van (2009). *Slachtofferschap van fraude: Een explorerend onderzoek naar de impact van diverse vormen van financieel-economische criminaliteit* [Fraud victimization: An exploratory study into the impact of diverse forms of financial crime]. International Victimology Institute Tilburg (INTERVICT).

Lai, F., Li, D. & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*(2), 353–363.

Lamet, W. & Wittebrood, K. (2009). *Nooit meer dezelfde: Gevolgen van misdrijven voor slachtoffers* [Never the same again: The consequences of crime for victims]. The Hague: The Netherlands Institute for Social Research (SCP).

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 1–10.

Lazarus, R. S. & Folkman, S. (1984). *Stress, appraisal, and coping*. New York: Springer Publishing Company.

Lee, D., Larose, R. & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445–454.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, *50*(2), 361–369.

Lee, Y. & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555.

Leukfeldt, E. R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering*, *4*(5), 26–32.

Leukfeldt, E. R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities.* The Hague: Eleven International (PhD thesis).

Leukfeldt, E. R. (Ed.). (2017). *Research agenda: The human factor in cybercrime and cybersecurity*. The Hague: Eleven International.

Leukfeldt, E. R., Kleemans, E. R. & Stol, W. P. (2017). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change*, 21–37.

Leukfeldt, E. R. & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behaviour*, *37*(3), 263–280.

Leventhal, H. (1970). Findings and theory in the study of fear communications. *Advances in Experimental Social Psychology*, *5*, 119–186.

Levi, M. & Burrows, J. (2008). Measuring the impact of fraud in the UK: A conceptual and empirical journey. *British Journal of Criminology*, *48*(3), 293–318.

Liang, H. & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71–90.

Liang, H. & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.

Lippke, S. & Ziegelmann, J. P. (2008). Theory-based health behavior change: Developing, testing, and applying theories for evidence-based interventions. *Applied Psychology: An International Review*, *57*(4), 698–716.

Ludl, C., McAllister, S., Kirda, E. & Kruegel, C. (2007). On the effectiveness of techniques to detect phishing sites. In *Proceedings of the 4th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 20–39).

Luo, X. R., Zhang, W., Burd, S. & Seazzu, A. (2012). Investigating phishing victimization with the heuristic-systematic model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28–38.

Maddux, J. E. & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479.

Maloney, E. K., Lapinski, M. K. & Witte, K. (2011). Fear appeals and persuasion: A review and update of the extended parallel process model. *Social and Personality Psychology Compass*, *5*(4), 206–219.

Mannan, M. & Oorschot, P. C. van (2008). Security and usability: The gap in real-world online banking. In *Proceedings of the 2007 Workshop on New Security Paradigms* (pp. 1–14).

Marinos, L. (2013). *ENISA threat landscape 2013: Overview of current and emerging cyber-threats*. Heraklion: European Union Agency for Network and Information Security.

Masurel, E. (2004). SMEs and crime evidence from the Netherlands. *International Small Business Journal*, *22*(2), 197–205.

Matthieu, M. M. & Ivanoff, A. (2006). Using stress, appraisal, and coping theories in clinical practice: Assessments of coping strategies after disasters. *Brief Treatment and Crisis Intervention*, *6*(4), 337.

Mayer, R. C., Davis, J. H. & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734.

McLaughlin, E. & Muncie, J. (2005). *The SAGE dictionary of criminology (second edition)*. SAGE Publications.

Meijnders, A. L., Midden, C. J. & Wilke, H. A. (2001). Communications about environmental risks and risk-reducing behavior: The impact of fear on information processing. *Journal of Applied Social Psychology*, *31*(4), 754–777.

Merton, R. K. (1968). *Social theory and social structure*. New York: The Free Press.

Michie, S., van Stralen, M. M. & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, *6*(1), 1–11.

Milne, S., Orbell, S. & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, *7*(2), 163–184.

Milne, S., Sheeran, P. & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143.

Moore, T. & Anderson, R. (2011). *Economics and internet security: A survey of recent analytical, empirical and behavioral research.* Retrieved from https://dash.harvard.edu/bitstream/handle/1/23574266/tr-03-11.pdf?sequence=1

Moser, A., Kruegel, C. & Kirda, E. (2007). Limits of static analysis for malware detection. In *Proceedings of the Computer Scurity Applications Conference* (pp. 421–430).

Murdoch, S. J., Drimer, S., Anderson, R. & Bond, M. (2010). Chip and PIN is broken. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy* (pp. 433–446).

Myers, L. & Abraham, C. (2005). Beyond 'doctor's orders'. *Psychologist*, *18*(11), 680–683.

NCSC (2015). *Cybersecuritybeeld Nederland (CSBN) 2015* [Cyber security assessment Netherlands (CSAN) 2015]. The Hague: National Cyber Security Centre.

NCSC (2016). *Cyber security assessment Netherlands (CSAN 2016)*. The Hague: National Cyber Security Centre.

NCTV (2013). *Nationale cyber security strategie 2: Van bewust naar bekwaam* [National cyber security strategy 2: From awareness to competence]. The Hague: National Coordinator for Security and Counterterrorism.

Ng, B.-Y., Kankanhalli, A. & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825.

Ngo, F. T. & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

Nhan, J., Kinkade, P. & Burns, R. (2009). Finding a pot of gold at the end of an Internet rainbow: Further examination of fraudulent email solicitation. *International Journal of Cyber Criminology*, *3*(1), 452–475.

Norberg, P. A., Horne, D. R. & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Norman, P., Boer, H. & Seydel, E. R. (2005). Protection motivation theory. In M. Conner & P. Norman (Eds.), *Predicting health behaviour* (pp. 81–126). Open University Press.

NVB (2013). *Position paper rondetafelgesprek online betalingsverkeer: 30 mei 2013* [Position paper on online banking: May 30, 2013]. Amsterdam: Dutch Banking Association.

O'Keefe, D. J. (2016). *Persuasion: Theory and research (third edition)*. Thousand Oaks: SAGE Publications.

Offenbeek, M. van, Boonstra, A. & Seo, D. (2013). Towards integrating acceptance and resistance research: Evidence from a telecare case study. *European Journal of Information Systems*, *22*(4), 434–454.

Ogden, J. (2003). Some problems with social cognition models: A pragmatic and conceptual analysis. *Health Psychology*, *22*, 424–428.

ONS (2016). *Crime in England and Wales: Year ending Sept 2016*. London: Office for National Statistics.

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the 40th Annual Hawaii International Conference on System Sciences* (p. 156–165).

Pallant, J. (2013). *SPSS survival manual: A step by step guide to data analysis using IBM SPSS*. Open University Press.

Parrish Jr, J. L., Bailey, J. L. & Courtney, J. F. (2009). *A personality based model for determining susceptibility to phishing attacks*. Oklahoma City, OK: Southwest Decision Sciences Institute.

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). *Human factors and information security: Individual, culture and security environment*. Edinburgh (Australia): Command, Control, Communications and Intelligence Division DSTO (Defence Science and Technology Organisation).

Pattinson, M., Jerram, C., Parsons, K., McCormac, A. & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*(1), 18–28.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, *7*(3), 101–134.

Peters, G.-J. Y., Ruiter, R. A. & Kok, G. (2013). Threatening communication: A critical re-analysis and a revised meta-analytic test of fear appeal theory. *Health Psychology Review*, *7*(sup1), S8–S31.

Petty, R. E. & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology* (pp. 123–205). New York: Academic Press.

Pleysier, S. (2011). Over objectieve en subjectieve onveiligheid. En de (on) zin van het rationaliteitdebat [On objective and subjective unsafety. And the (non) sense of the rationality debate]. *Tijdschrift voor Veiligheid*, *10*(4), 24–40.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y. & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

Ponemon Institute (2012). *The impact of cybercrime on business: Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil*. Ponemon Institute Research Report.

Posey, C., Roberts, T. L. & Lowry, P. B. (2015). The impact of organizational commitment on insiders' notivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214.

Pratt, T. C., Holtfreter, K. & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296.

Prentice-Dunn, S. & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research*, *1*(3), 153–161.

Prochaska, J. O., Wright, J. A. & Velicer, W. F. (2008). Evaluating theories of health behavior change: A hierarchy of criteria applied to the transtheoretical model. *Applied Pyschology: An International Review*, *57*, 561-588.

Purkait, S. (2012). Phishing counter measures and their effectiveness - Literature review. *Information Management & Computer Security*, *20*(5), 382–420.

Purkait, S., Kumar De, S. & Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. *Information Management & Computer Security*, *22*(3), 194–234.

PwC (2013). *Naar een fraudebeeld Nederland* [Towards a fraud assessment of the Netherlands]. Amsterdam: PricewaterhouseCoopers.

Reyns, B. W., Henson, B. & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169.

Rhee, H.-S., Kim, C. & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826.

Ringle, C. M., Wende, S. & Will, A. (2005). *SmartPLS 2.0.M3*. Retrieved from http://www.smartpls.com

Ritchie, J., Lewis, J., McNaughton-Nicholls, C. & Ormston, R. (2014). *Qualitative research practice: A guide for social science students & researchers*. London, UK: SAGE Publications.

Rocha Flores, W., Holm, H., Svensson, G. & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security*, *22*(4), 393–406.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114.

Rosenstock, I. M., Stretcher, V. J. & Becker, M. H. (1988). Social learning theory and the health belief model. *Health Education Quarterly*, *15*(2), 175–183.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, *80*(1), 1–28.

Rousseau, D. M., Sitkin, S. B., Burt, R. S. & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404.

Ruiter, R. A. C., Kessels, L. T. E., Peters, G.-J. Y. & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, *49*(2), 63–70

Sam, H. K., Othman, A. E. A. & Nordin, Z. S. (2005). Computer self-efficacy, computer anxiety, and attitudes toward the internet: A study among undergraduates in Unimas. *Journal of Educational Technology & Society*, *8*(4), 205–219.

Sasse, M. A., Brostoff, S. & Weirich, D. (2001). Transforming the "weakest link" – A human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131.

Savage, I. (1993). Demographic influences on risk perceptions. *Risk Analysis*, *13*(4), 413–420.

Schaik, P. van, Jeske, D., Onibokun, J., Coventry, L., Jansen, J. & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559.

Schaper, M. T. & Weber, P. (2012). Understanding small business scams. *Journal of Enterprising Culture*, *20*(03), 333–356.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. New York: John Wiley & Sons.

Schoepfer, A. & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, *37*(2), 209–215.

Shapland, J. & Hall, M. (2007). What do we know about the effects of crime on victims? *International Review of Victimology*, *14*(2), 175–217.

Sharma, K., Singh, A. & Sharma, V. P. (2009). SMEs and cybersecurity threats in e-commerce. *EDPACS: The EDP Audit, Control, and Security Newsletter*, *39*(5-6), 1–49.

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J. & Hutton, S. (2003). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Science*, *49*(1), 1–6.

Sheeran, P. (2002). Intention–behavior relations: A conceptual and empirical review. *European Review of Social Psychology*, *12*(1), 1–36.

Sheeran, P., Harris, P. R. & Epton, T. (2014). Does heightening risk appraisals change people's intentions and behavior? A meta-analysis of experimental studies. *Psychological Bulletin*, *140*(2), 511–543.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382).

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R. & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207.

Shneiderman, B. (2000). Designing trust into online experiences. *Communications of the ACM*, *43*(12), 57–59.

Shover, N., Fox, G. L. & Mills, M. (1994). Long-term consequences of victimization by white-collar crime. *Justice Quarterly*, *11*(1), 75–98.

Sjöberg, L. (2000). Factors in risk perception. *Risk Analysis*, *20*(1), 1–11.

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280–285.

Slovic, P., Fischhoff, B. & Lichtenstein, S. (1982). Why study risk perception? *Risk Analysis*, *2*(2), 83–93.

Slovic, P. & Peters, E. (2006). Risk perception and affect. *Current Directions in Psychological Science*, *15*(6), 322–325.

Spiekermann, S., Grossklags, J. & Berendt, B. (2001). E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce* (pp. 38–47).

Sommestad, T., Karlzén, H. & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, *23*(2), 200–217.

Starr, C. (1969). Social benefit versus technological risk. *Science*, *165*, 1232–1238.

Statline (2013). *Beroepsbevolking: Behaalde onderwijs naar persoonskenmerken 2001-2012* [Working population: Level of education by personal characteristics 2001-2012]. Retrieved from http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=71822NED&D1=0&D2=a&D3=a&D4=0-1,4&D5=a&D6=0&D7=2,l&HD=130926-1540&HDR=T,G3,G5,G6,G1&STB=G2,G4

Statline (2015). *Beroepsbevolking: Kerncijfers* [Working population: Key figures]. Retrieved from http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=37296ned&D1=a&D2=0,10,20,30,40,50,60,(l-1),l&HD=130605-0924&HDR=G1&STB=T

Statline (2016a). *Bevolking; geslacht, leeftijd en burgerlijke staat, 1 januari* [Population; gender, age and marital status, 1 January]. Retrieved from http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=7461BEV&D1=0&D2=0&D3=0-100,122-129&D4=0,10,20,30,40,50,l&HDR=T,G3&STB=G1,G2&VW=T

Statline (2016b). *Internet faciliteiten; particuliere huishoudens* [Internet facilities; private households]. Retrieved from http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83291NED&D1=a&D2=0-5&D3=0&D4=a&VW=T

Statline (2017a). *Arbeidsdeelname: Kerncijfers* [Rate of employement: Key figures]. Retrieved from http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLnl&PA=82309NED&LA=nl

Statline (2017b). *Bevolking: Hoogst behaald onderwijsniveau; geslacht, leeftijd en herkomst* [Population: Hightest attained level of education; gender, age and origin]. Retrieved from http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLnl&PA=82275NED&LA=nl

Statline (2017c). *Bevolking: Kerncijfers* [Population: Key figures]. Retrieved from http://statline.cbs.nl/StatWeb/publication/?PA=37296ned&D1=a&D2=0,10,20,30,40,50,60,(l-1),l&HDR=G1&STB=T

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13*(2), 147–169.

Sutton, M. (2009). Product design: CRAVED and VIVA. In B. S. Fisher & S. P. Lab (Eds.), *Encyclopedia of victimology and crime prevention*. Thousand Oaks: SAGE.

Tam, L., Glassman, M. & Vandenwauver, M. (2010). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology*, *29*(3), 233–244.

Tan, M. & Sagala Aguilar, K. (2012). An investigation of students' perception of Bluetooth security. *Information Management & Computer Security*, *20*(5), 364–381.

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K. & Albarracín, D. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin*, *141*(6), 1178–1204.

Tanner, J. F., Hunt, J. B. & Eppright, D. R. (1991). The protection motivation model: A normative model of fear appeals. *The Journal of Marketing*, 36–45.

Taylor, S. E., Wood, J. V. & Lichtman, R. R. (1983). It could be worse: Selective evaluation as a response to victimization. *Journal of Social Issues*, *39*(2), 19–40.

Thaler, R. H. & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth and happiness*. London, UK: Penguin Group.

Torkzadeh, G. & Koufteros, X. (1994). Factorial validity of a computer self-efficacy scale and the impact of computer training. *Educational and Psychological Measurement*, *54*(3), 813–821.

Tsow, A. & Jakobsson, M. (2007). *Deceit and deception: A large user study of phishing.* Retrieved from http://www.cs.indiana.edu/pub/techreports/TR649.pdf

Tu, Z. & Yuan, Y. (2012). Understanding user's behaviors in coping with security threat of mobile devices loss and theft. In *Proceedings of the 45th Hawaii International Conference on System Science* (pp. 1393–1402).

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*, 190–198.

Veenstra, S., Zuurveen, R. & Stol, W. (2015). *Cybercrime onder bedrijven: Een onderzoek naar slachtofferschap van cybercrime onder het midden- en kleinbedrijf en zelfstandigen zonder personeel in Nederland* [Cybercrime among companies: Research into cybercrime victimization among small and medium-sized enterprises and one-man businesses in the Netherlands]. Leeuwarden: Cybersafety Research Group.

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478.

Vilares, M. J., Almeida, M. H. & Coelho, P. S. (2010). Comparison of likelihood and PLS estimators for structural equation modeling: A simulation with customer satisfaction data. In V. Esposito Vinzi, W.W. Chin, J. Henseler, & H. Wang (Eds.), *Handbook of partial least squares: Concepts, methods and application* (pp. 289–306). Berlin: Springer.

Vishwanath, A., Harrison, B. & Ng, Y. J. (2016). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research*, *online preprint*, 1–21.

Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576–586.

Vlaev, I., Chater, N. & Stewart, N. (2009). Dimensionality of risk perception: Factors affecting consumer understanding and evaluation of financial risk. *Journal of Behavioral Finance*, *10*(3), 158–181.

Wall, D. S. (2008). Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society*, *11*(6), 861–884.

Wall, J. D. & Buche, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems*, *41*, 277–300.

Wang, J., Chen, R., Herath, T. & Rao, H. R. (2009). Visual e-mail authentication and identification services: An investigation of the effects on e-mail use. *Decision Support Systems*, *48*(1), 92–102.

Wash, R. (2010). Folk models of home computer security. In *Proceedings of the 6th Symposium on Usable Privacy and Security* (pp. 1–16).

WEF (2016). *The global risks report 2016: 11th edition*. Geneva: World Economic Forum.

Weinstein, N. D. (1993). Testing four competing theories of health-protective behavior. *Health Psychology*, *12*(4), 324–333.

Wemmers, J.-A. (2013). Victims' experiences in the criminal justice system and their recovery from crime. *International Review of Victimology*, *19*(3), 221–233.

West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34–40.

Whitty, M. T. & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims-both financial and non-financial. *Criminology and Criminal Justice*, *16*(2), 176–194.

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, *17*(3), 131–132.

Wijn, R., van den Berg, H., Wetzer, I. M. & Broekman, C. C. M. T. (2016). *Supertargets: Verkenning naar voorspellende en verklarende factoren voor slachtofferschap van cybercriminaliteit* [Super targets: Exploration of predictive and explanatory factors for cybercrime victimization]. Soesterberg: TNO.

Williams, M. L. (2015). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*, 21–48.

Wilsem, J. van (2011a). "Bought it, but never got it": Assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178.

Wilsem, J. van (2011b). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115–127.

Wilsem, J. van, Meulen, N. van der & Kunst, M. (2013). Je geld kwijt, en dan [Lost your money, and then what]? *Tijdschrift voor Criminologie*, *55*(4), 360–374.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329–349.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs*, *61*(2), 113–134.

Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, *1*, 317–341.

Witte, K. & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior*, *27*(5), 591–615.

Witte, K., Berkowitz, J. M., Cameron, K. A. & McKeon, J. K. (1998). Preventing the spread of genital warts: Using fear appeals to promote self-protective behaviors. *Health Education & Behavior*, *25*(5), 571–585.

WODC & TNS NIPO (2011). *Monitor Criminaliteit Bedrijfsleven 2010: Feiten en trends inzake aard en omvang van criminaliteit in het bedrijfsleven* [Crime Monitor Businesses 2010: Facts and trends related to the nature and extent of crime among businesses]. Amsterdam: TNS NIPO.

Workman, M., Bommer, W. H. & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816.

Workman, M., Bommer, W. H. & Straub, D. (2009). The amplification effects of procedural justice on a threat control model of information systems security behaviours. *Behaviour & Information Technology*, *28*(6), 563–575

Wu, M., Miller, R. C. & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 601–610).

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.

Yoon, C., Hwang, J.-W. & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, *23*(4), 407–415.

Yousafzai, S. Y., Foxall, G. R. & Pallister, J. G. (2010). Explaining internet banking behavior: Theory of reasoned action, theory of planned behavior, or technology acceptance model? *Journal of Applied Social Psychology*, *40*(5), 1172–1202

Yousafzai, S. Y., Pallister, J. G. & Foxall, G. R. (2003). A proposed model of e-trust for electronic banking. *Technovation*, *23*(11), 847–860.

Yousafzai, S. Y., Pallister, J. G. & Foxall, G. R. (2009). Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal*, *29*(5), 591–605.

Yousafzai, S. Y. & Yani-de-Soriano, M. (2012). Understanding customer-specific factors underpinning internet banking adoption. *International Journal of Bank Marketing*, *30*(1), 60–81.

Zhao, X., Lynch, J. G. & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, *37*(2), 197–206.

Zhou, T. (2012). Understanding users' initial trust in mobile banking: An elaboration likelihood perspective. *Computers in Human Behavior*, *28*(4), 1518–1525.

Zimmerman, M. A. (1995). Psychological empowerment: Issues and illustrations. *American Journal of Community Psychology*, *23*(5), 581–599.

Appendix I: Outline research program

The Dutch Research Program on Safety and Security of Online Banking started in April 2012 and ended on October 2017, and was funded by the Dutch Banking Association, the Police Academy of the Netherlands and the Dutch National Police. The goals of this multidisciplinary research program were to contribute to the safety and security of online banking and to advance scientific knowledge and theory in this area. A multidisciplinary perspective was necessary because online banking fraud is a complex, societal problem that cannot be solved by a simple, monodisciplinary solution.[68]

Within the research program, four different perspectives were taken on tackling the problem of online banking fraud. All were designed as PhD studies. The first study, which is presented in this thesis, is conducted from a behavioural information security perspective and dealt with the question of how end users can be made more resilient to online banking fraud. The second study, which took a criminology perspective, dealt with the question how cybercriminal networks that carry out phishing and malware attacks can be disrupted.[69] The third study adopted a technical security approach and dealt with the question of how online banking transactions can most effectively be secured from a technical and usable perspective.[70] The fourth and final study was conducted from a socio-legal perspective and was concerned with detection, investigation and prosecution of online banking fraud. In particular, it dealt with the question of how the public-private fight against online banking fraud can be designed effectively.[71]

The knowledge institutes involved with the research program are the Cybersafety Research Group from NHL Stenden University of Applied Sciences and the Police Academy of the Netherlands, and the Open University of the Netherlands.

---

[68] Stol, W. Ph., Eekelen, M. van, Stamhuis, E., & Kop, N. (2011). *Veiligheid digitaal betalingsverkeer: Presentatie van een verbetergericht kennisprogramma* [Improving the safety and security of digital payment systems: Presentation of a knowledge program]. Leeuwarden: Open University of the Netherlands, NHL Stenden University of Applied Sciences and the Police Academy of the Netherlands.

[69] Leukfeldt, E. R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. The Hague: Eleven International (PhD thesis).

[70] Kiljan, S. (2017). *Exploring, expanding and evaluating usable security in online banking*. Heerlen: Open University of the Netherlands (PhD thesis).

[71] Boes, S. (work in progress). See for updates: https://cybersciencecenter.nl

Appendix II: Interview data

Table AII.1: Short summary of the interviews

Inter-view	Gender	Age (years)	Level of education	Victim type	Fraud type	Damage (euros)	Reimbursed
01	Female	58	Medium	Private	Phishing	13,000	Yes
02	Female	79	Medium	Private	Phishing	2,000	Yes
03	Male	45	Medium	Private	Phishing	11,000	Yes
04	Male	89	High	Private	Phishing	2,000(a)	N/a
05	Male	73	Medium	Private	Phishing	8,000	Yes
06	Female	59	High	Private	Phishing	3,600	1,000
07	Male	77	Low	Private	Phishing	10,000(a)	N/a
08	Female	70	High	Private	Phishing	50,000	Yes
09	Male	36	Medium	Corporate	Malware	1,300	Yes
10	Male	68	Medium	Corporate	Phishing	900	Yes
11	Male	23	High	Private	Phishing	7,000	Yes
12	Female	74	Low	Private	Phishing	1,200	No
13	Female	73	Low	Private	Phishing	1,800	No
14	Male	80	High	Private	Phishing	4,800	Yes (-150)
15	Female	74	High	Private	Phishing	50,000	No
16	Male	67	Medium	Private	Phishing	2,500	Yes (-150)
17	Male	71	Medium	Private	Phishing	5,700	No
18	Female	61	High	Private	Phishing	20,000	Yes (-150)
19	Male	38	High	Corporate	Malware	M.w.(a)	N/a
20	Female	64	Medium	Corporate	Malware	6,900	Yes
21	Male	29	Medium	Corporate	Malware	10,00	Yes
22	Female	57	Medium	Corporate	Malware	5,000	Yes
23	Female	46	Medium	Corporate	Malware	4,700	Yes
24	Male	64	High	Corporate	Malware	3,000	Yes
25*	Female	56	High	Corporate	Malware	5,000	Yes
26	Male	31	Medium	Private	Malware	3,500	Yes
27	Male	30	Medium	Corporate	Malware	4,700	Yes
28*	Male	63	High	Corporate	Malware	5,000	Yes
29	Male	50	High	Corporate	Malware	3,700	Yes
30	Female	51	Medium	Corporate	Malware	N.t.	Yes

*Note. *: not the actual victim. a: attempt. m.w.: about a monthly wage. n.t.: not told. n/a: not applicable. -150: minus mandatory own risk (i.e., 150 euros).*

Appendix III: Instrument private customers

Table A.III.1: Instrument (translated from Dutch)

Construct (sources)	Items	
Perceived vulnerability (Witte, 1996)	PV1:	I am at risk for being victimized by online banking fraud
	PV2:	It is likely that I will become victim of online banking fraud
	PV3:	It is possible that I will become victim of online banking fraud
Perceived severity (Witte, 1996)	PS1:	I believe that online banking fraud is a severe problem
	PS2:	I believe that online banking fraud is a serious problem
	PS3:	I believe that online banking fraud is a significant problem
Perceived risk (Grabner-Kräuter & Faullant, 2008)	PR1:	I am afraid of being victimized by online banking fraud
	PR2:	I believe it can rather easily happen that criminals steal money during online banking sessions
	PR3:	I am afraid that others can access my online bank account without my permission
Trust in online Banking (Yousaf--zai et al., 2009)	TR1:	I trust online banking
	TR2:	I trust my bank
	TR3:	I trust the internet for banking transactions
Response efficacy (Witte, 1996)	RE1:	The uniform safety rules help in preventing online banking fraud
	RE2:	Complying with the uniform safety rules is effective in preventing online banking fraud
	RE3:	If I follow the uniform safety rules, I am less likely to be victimized by online banking fraud
Self-efficacy (Witte, 1996)	SE1:	I am able to comply with the uniform safety rules
	SE2:	The uniform safety rules are easy to follow
	SE3:	Following the uniform safety rules is convenient
Response costs (Ng et al., 2009)	RC1:	Following the uniform safety rules is time-consuming
	RC2:	Complying with the uniform safety rules requires a lot of mental effort
	RC3:	Complying with the uniform safety rules would require starting a new habit
Injunctive norms (Anderson & Agarwal, 2010)	IN1:	Friends who influence my behaviour would think that I should take safety measures to protect myself against online banking fraud
	IN2:	Significant others who are important to me would think that I should take safety measures to protect myself against online banking fraud
	IN3:	My peers would think that I should take safety measures to protect myself against online banking fraud
Descriptive norms (Anderson & Agarwal, 2010; Herath & Rao, 2009)	DN1:	I believe other people implement security measures to protect themselves against online banking fraud
	DN2:	I am convinced other people take security measures to protect themselves against online banking fraud
	DN3:	The majority of people who make use of online banking take security measures to protect themselves against online banking fraud

Table A.III.1 (continued): Instrument (translated from Dutch)

Construct (sources)	Items	
Locus of control (Workman et al., 2008, 2009)	LoC1:	Keeping online banking safe is within my control
	LoC2:	I believe that it is within my control to protect myself against online banking fraud
	LoC3:	The primary responsibility for protecting me against online banking fraud belongs to me
Protection motivation (Anderson & Agarwal, 2010; Herath & Rao, 2009; Ifinedo, 2012)	PM1:	I am likely to follow the uniform safety rules to protect myself against online banking fraud
	PM2:	I am willing to comply with the uniform safety rules to protect myself against online banking fraud
	PM3:	I am certain that I will follow the uniform safety rules to protect myself against online banking fraud
	PM4:	It is my intention to comply with the uniform safety rules
Online banking experience (Corbitt et al., 2003)	OBX1:	I have been using online banking for: (less than 1 year/between 1 and 5 years/between 6 and 10 years/between 11 and 15 years/more than 15 years)
	OBX2:	I use online banking to check my account balance approximately: ((almost) daily/ at least once per week/ at least twice per week/ at least once per month/less than once a month)
	OBX3:	I use online banking to make payments to third parties approximately: ((almost) daily/ at least once per week/ at least twice per week/ at least once per month/less than once a month)
	OBX4:	I perceive myself experienced at using online banking (1 strongly disagree – 5 strongly agree)

Note. Only OBX4 was used as a measure for online-banking experience in the structural models.

Factor loadings – original measurement model (Chapter 7)

The factor loadings are presented in Table A.III.2 and show that most items loaded on their corresponding factor and had no cross-loadings. Exceptions were the items Attitude 2 and Attitude 3 (loading highly on om the factor protection motivation), Habit 1 (loading highly on the factor protection motivation), Habit 2 (with a low loading on the factor habit), Protection Motivation 1-4 (loading highly on the factor attitude), Response Costs 3 (with a poor loading on the factor response costs), Self-efficacy 1 (loading highly on the factor protection motivation) and Self-efficacy 3 (loading highly on the factors protection motivation and habit). Because of these results, the factors attitude and habit as well as their items (see Table A.III.2) were removed from any subsequent analysis. The factor self-efficacy was retained, as it is an important component in protection motivation theory. However, because of their cross-loadings, the items Self-efficacy 1 and Self-efficacy 3 were removed. Because of low loadings, the item Response Costs 3 was also removed. The items for attitude and habit are presented in Table A.III.3.

Table A.III.2: Component loadings – original measurement model

	PV	PS	PR	TR	RE	SE	RC	IN	DN	AT	LoC	PM	HA
PV1	**0.89**	0.17	0.63	-0.33	-0.26	-0.24	0.24	0.17	-0.02	-0.15	-0.27	-0.17	-0.19
PV2	**0.91**	0.22	0.69	-0.35	-0.28	-0.28	0.28	0.22	0.02	-0.18	-0.29	-0.20	-0.20
PV3	**0.72**	0.21	0.55	-0.24	-0.17	-0.15	0.12	0.11	-0.01	-0.06	-0.20	-0.09	-0.17
PS1	0.22	**0.86**	0.27	-0.08	0.06	0.16	-0.04	0.04	0.12	0.24	0.07	0.22	0.17
PS2	0.13	**0.87**	0.20	-0.03	0.11	0.25	-0.11	-0.05	0.09	0.31	0.09	0.28	0.21
PS3	0.26	**0.88**	0.37	-0.12	0.05	0.14	0.01	0.07	0.11	0.25	0.03	0.21	0.15
PR1	0.60	0.30	**0.85**	-0.38	-0.23	-0.21	0.27	0.21	0.05	-0.08	-0.23	-0.09	-0.17
PR2	0.68	0.21	**0.81**	-0.37	-0.32	-0.26	0.25	0.16	-0.03	-0.19	-0.29	-0.20	-0.21
PR3	0.61	0.30	**0.87**	-0.40	-0.26	-0.25	0.25	0.16	0.01	-0.11	-0.30	-0.13	-0.20
TR1	-0.35	-0.11	-0.45	**0.90**	0.40	0.29	-0.19	-0.03	0.15	0.23	0.42	0.24	0.22
TR2	-0.26	-0.01	-0.29	**0.82**	0.43	0.28	-0.20	0.01	0.22	0.29	0.45	0.29	0.23
TR3	-0.33	-0.10	-0.41	**0.83**	0.35	0.23	-0.14	0.01	0.16	0.18	0.35	0.19	0.18
RE1	-0.25	0.08	-0.29	0.39	**0.89**	0.60	-0.32	0.00	0.33	0.65	0.59	0.64	0.48
RE2	-0.23	0.03	-0.24	0.43	**0.77**	0.47	-0.17	0.08	0.28	0.54	0.56	0.48	0.38
RE3	-0.25	0.10	-0.28	0.36	**0.88**	0.59	-0.33	-0.02	0.33	0.65	0.61	0.66	0.52
SE1	-0.24	0.19	-0.26	0.29	0.58	**0.89**	-0.46	-0.13	0.21	0.64	0.54	0.71	0.65
SE2	-0.24	0.18	-0.24	0.26	0.57	**0.87**	-0.42	-0.08	0.25	0.65	0.51	0.65	0.65
SE3	-0.24	0.20	-0.25	0.29	0.61	**0.91**	-0.51	-0.10	0.30	0.67	0.58	0.75	0.79
RC1	0.23	-0.07	0.25	-0.19	-0.29	-0.49	**0.90**	0.31	-0.02	-0.40	-0.31	-0.40	-0.39
RC2	0.24	0.00	0.30	-0.17	-0.25	-0.40	**0.85**	0.34	-0.02	-0.27	-0.23	-0.30	-0.29
RC3	0.10	0.12	0.14	0.05	0.19	0.05	**0.14**	0.22	0.20	0.18	0.15	0.14	0.01
IN1	0.17	0.03	0.16	0.01	0.05	-0.05	0.25	**0.88**	0.20	-0.01	0.06	0.01	0.01
IN2	0.20	0.02	0.22	-0.02	-0.02	-0.14	0.36	**0.87**	0.13	-0.06	-0.03	-0.09	-0.08
IN3	0.17	0.02	0.16	0.01	0.03	-0.09	0.30	**0.90**	0.18	-0.05	0.03	-0.03	-0.03
DN1	0.02	0.13	0.04	0.17	0.32	0.28	-0.06	0.12	**0.87**	0.29	0.27	0.31	0.28
DN2	0.00	0.09	0.02	0.17	0.30	0.20	0.00	0.19	**0.86**	0.27	0.29	0.29	0.25
DN3	-0.03	0.10	-0.03	0.19	0.34	0.27	-0.04	0.19	**0.88**	0.30	0.30	0.33	0.32
AT1	-0.17	0.23	-0.15	0.28	0.65	0.65	-0.37	-0.04	0.27	**0.87**	0.50	0.68	0.50
AT2	-0.11	0.30	-0.09	0.19	0.64	0.63	-0.33	-0.02	0.34	**0.90**	0.51	0.75	0.60
AT3	-0.16	0.29	-0.16	0.27	0.67	0.70	-0.38	-0.06	0.29	**0.92**	0.55	0.82	0.62
LoC1	-0.26	0.13	-0.27	0.40	0.61	0.56	-0.30	-0.02	0.26	0.54	**0.83**	0.56	0.47
LoC2	-0.27	0.04	-0.28	0.39	0.56	0.53	-0.25	0.03	0.28	0.46	**0.81**	0.49	0.47
LoC3	-0.17	0.02	-0.20	0.35	0.52	0.39	-0.19	0.08	0.29	0.41	**0.77**	0.41	0.36
PM1	-0.14	0.22	-0.12	0.22	0.58	0.66	-0.36	-0.03	0.32	0.71	0.49	**0.88**	0.60
PM2	-0.19	0.25	-0.16	0.26	0.65	0.69	-0.36	-0.02	0.32	0.72	0.53	**0.90**	0.61
PM3	-0.18	0.26	-0.15	0.26	0.64	0.76	-0.40	-0.04	0.34	0.73	0.56	**0.90**	0.75
PM4	-0.16	0.25	-0.16	0.26	0.66	0.72	-0.39	-0.07	0.29	0.83	0.55	**0.90**	0.65
HA1	-0.19	0.19	-0.20	0.24	0.53	0.76	-0.40	-0.05	0.30	0.63	0.50	0.72	**0.92**
HA2	-0.10	0.08	-0.13	0.11	0.20	0.35	-0.17	-0.03	0.19	0.23	0.22	0.30	**0.60**
HA3	-0.22	0.20	-0.22	0.23	0.53	0.73	-0.36	-0.03	0.30	0.60	0.52	0.68	**0.90**

Note. PV: perceived vulnerability. PS: perceived severity.PR: perceived risk. TR: trust. RE: response efficacy. SE: self-efficacy. RC: response costs. IN: injunctive norms. DN: descriptive norms. AT: attitude. LoC: locus of control. PM: protection motivation. HA: habit.

Table A.III.3: Additional items from initial instrument (translated from Dutch)

Construct / sources	Items	
Attitude (Anderson & Agarwal, 2010; Ifinedo, 2012)	AT1: AT2: AT3:	Following the uniform safety rules is a good idea Complying with the uniform safety rules is a necessity Following the uniform safety rules is important
Habit (Vance et al., 2012)	HA1: HA2: HA3:	Complying with the uniform safety rules is something I do automatically Complying with the uniform safety rules is something I do without having to consciously remember to do so Complying with the uniform safety rules is something that belongs to my routine

Appendix IV: Instrument corporate customers

Table A.IV.1: Questionnaire items, scales, means, and standard deviations (translated from Dutch; N = 1,622)

Variables	Items	Scale	M	*SD*
Protection motivation				
Technical coping measures	-The business computer(s) is equipped with anti-virus software	(1) yes, (2) no, (3) do not know	1.09	.342
	-The business computer(s) is equipped with a firewall		1.16	.501
	-The (wireless) network connecting the business computer(s) is secured		1.15	.502
	-The software running on the business computer(s) is continuously updated		1.13	.448
Personal coping measures	-I have adopted rules for safe online banking	(1) yes, (2) no, (3) do not know	1.21	.461
	-I have adopted rules for handling sensitive data (such as customer data)		1.21	.481
	-I have adopted rules for opening potentially untrusted files (such as e-mail attachments)		1.08	.327
	-I have adopted rules for sharing sensitive information to third parties		1.10	.343
Threat appraisal				
Perceived risk	-I am worried about online threats	(1) totally disagree – (4) totally agree	2.15	.753
Coping appraisal PMT				
Response efficacy	-How confident are you in the measures taken to prevent online threats	(1) very little/ no confidence – (5) a lot of confidence	2.44	.686
Self-efficacy	To what extent do you poses the following digital skills:	(1) to a very small extent – (4) to a very large extent		
	-I can organise and manage computer files (open, save, copy, move, organise them in folders)		3.43	.830
	-I can find files using the search function on my computer		3.47	.731
	-I know most of the software functions on the computer		3.09	.907
	-I can install software		3.02	1.059
	-I can boot software on my computer		3.28	.875
	-I can use most software on my computer, like Word, Excel and PowerPoint		3.32	.867
	-If a program is not working, I understand why		2.63	.976
	-I can solve computer problems		2.49	.994
	-I know most of the hardware functions on my computer		2.69	1.001
	-I can use computer (related) hardware, such as CD / DVD drives, USB ports, scanners and printers		3.26	.845
	-I can use a web browser, for example, to search for information		3.48	.711

Table A.IV.1 (continued): Questionnaire items, scales, means, and standard deviations (translated from Dutch; N = 1,622)

Variables	Items	Scale	M	*SD*
Self-efficacy (continued)	To what extent do you poses the following digital skills:	(1) to a very small extent –		
	-I can communicate with others via the internet, for example, by e-mail or via chat applications	(4) to a very large extent	3.49	.718
	-I can create a web page		2.17	1.211
	-I can use programming languages		1.65	1.027
Coping appraisal added				
Attitude	-How important is information security for your business?	(1) very unimportant – (5) very important	2.12	.895
Locus of control	-I am responsible for my own online safety	(1) totally disagree – (5) totally agree	1.67	.773
Additional variables				
Prior internet experience	-On average, how many hours a day do you spent online (private and business purposes combined)?	(1) 0-2 hours – (5) more than 8 hours	2.32	1.307
Prior victimization	-Has your business ever been victim of a malware attack?	(1) do not know, (2) no,	2.55	.959
	-Has your business ever been victim of a phishing attack?	(3) one or more failed attempts, (4) victimized once, (5) victimized several times	2.50	.773
IT dependence	-How dependent is your business of computers and internet (IT)?	(1) not at all dependent – (7) completely dependent	3.02	1.690
Confidential information	-To what extent is confidential information (such as customer data) stored on your business computer(s)?	(1) none – (6) to a very large extent	2.99	1.581

Appendix V: Instrument internet users

Text box A.V.1: Strong-fear appeal message (translated from Dutch)

Phishing is increasingly prevalent in the Netherlands and is a common form of online fraud. Research by Statistics Netherlands shows that phishing victimization in the Netherlands occurs in walks of life. Recent scientific research reveals that up to 45% of all people fall for phishing attacks. The chances of getting phished – or already having experienced it – are thus very real.

Phishing attacks are becoming more sophisticated and thus appear more credible. Whereas phishing e-mails could previously be recognized by spelling mistakes, now-a-days, they look very much like the original mails that are sent by the organization that criminals imitate, are written in proper Dutch and are more personalized. This means that it becomes more difficult to recognize phishing attempts and, therefore, more probable to fall victim to it. When criminals acquire your personal information, they take over your identity with which they perform all kinds of harmful practices such as robbing your bank account and purchasing products on your behalf for which they do not pay.

A phishing attack often starts with receiving a phishing e-mail. A simple and effective way to counter phishing is to be extra careful when handing over your personal information so that you are not at risk of receiving phishing e-mails. A specific measure that you can take is that you do not share this information online with others, for example, on social media (Facebook, LinkedIn, etc.), on your personal website or when a website asks for it. Research has shown that by taking this simple measure you can prevent a phishing attack on your behalf, or an attack on you will be in vain. Of course, you may need to share such information, for example, when making purchases on a trusted web shop. The fact remains that you have to deal with your personal information carefully. After all, when you do not meet the recommended measure, you run a very high risk of getting phished.

Text box A.V.2: Weak-fear appeal message (translated from Dutch)

Phishing is a type of online fraud in which people are scammed. Research by Statistics Netherlands shows that 0.4% of the Dutch population has been a victim of phishing in the previous year. Recent scientific research reveals that at least 3% of all people fall for phishing attacks. Therefore, there is a possibility that you will also get phished or that you already have experienced it.

Criminals always find new phishing methods to gain personal information. When criminals acquire such data, they can take over one's identity, for example, to plunder bank accounts or purchase products for which they do not pay. Although the risk of becoming a victim of phishing is small according to research, this can have adverse consequences.

A phishing attack often starts with receiving a phishing e-mail. A simple and effective way to counter phishing is to be extra careful when handing over your personal information so that you are not at risk of receiving phishing e-mails. A specific measure that you can take is that you do not share this information online with others, for example, on social media (Facebook, LinkedIn, etc.), on your personal website or when a website asks for it. Research has shown that by taking this simple measure you can prevent a phishing attack on your behalf, or an attack on you will be in vain. Of course, you may need to share such information, for example, when making purchases on a trusted web shop. The fact remains that you have to deal with your personal information carefully. After all, when you do not meet the recommended measure, there is a chance of getting phished.

Table A.V.1: Instrument (translated from Dutch)

Construct (sources)	Items	
Perceived vulnerability (Witte, 1996)	PV1:	It is likely that I will become victim of phishing
	PV2:	I am at risk for being victimized by phishing
	PV3:	It is possible that I will become victim of phishing
Perceived severity (Johnston et al., 2015; Witte, 1996)	PS1:	If I was a victim of phishing, the consequences would be severe
	PS2:	If I was a victim of phishing, the consequences would be serious
	PS3:	If I was a victim of phishing, the consequences would be significant
Fear (Milne et al., 2002)	FE1:	The thought of becoming a phishing victim makes me feel frightened
	FE2:	The thought of becoming a phishing victim makes me scared
	FE3:	I am anxious about the prospect of becoming a victim of phishing
	FE4:	I am worried about the prospect of becoming a victim of phishing
Response efficacy (Witte, 1996)	RE1:	If I do no share personal information online, then that helps to prevent phishing
	RE2:	I think that not sharing personal information online is an effective means to counter phishing attacks
	RE3:	If I do no share personal information online, then I think the chance decreases of becoming a victim of phishing

Table A.V.1 (continued): Instrument (translated from Dutch)

Construct (sources)	Items	
Self-efficacy (Witte, 1996)	SE1:	I am able to apply the measure of not sharing personal information online to my internet behaviour in order to prevent phishing
	SE2:	The measure of not sharing personal information online is easy to use to prevent phishing
	SE3:	Using the recommended measure to not share personal information online to prevent phishing is convenient
Response costs (Ng et al., 2009)	RC1:	Not sharing personal information online is inconvenient
	RC2:	Exercising care when deciding whether or not to share personal information online is time-consuming
	RC3:	Not sharing personal information online requires a lot of mental effort
	RC4:	Not sharing personal information online would require starting a new habit, which is difficult
Protection motivation (Anderson & Agarwal, 2010; Ifinedo, 2012)	PM1:	I am likely to take the measure of not sharing personal information online to protect myself against phishing attacks, for the next month
	PM2:	I would follow the measure of not sharing personal information online to protect myself against phishing attacks, for the next month
	PM3:	I am certain to take the measure of not sharing personal information online to protect myself against phishing attacks, for the next month
	PM4:	It is my intention to take the measure of not sharing personal information online, for the next month
Resistance (Witte, 1994; Witte et al., 1998)	RS1:	Based on what I have read, I do not think it is necessary to protect myself against phishing
	RS2:	After reading the text, I had no inclination to do something against phishing
	RS3:	I think it is unnecessary to protect myself from phishing, even after reading the text
Avoidance (Brouwers & Sorrentino, 1993; Witte et al., 1998)	AV1:	When I read the text, my first instinct was to not want to think about the possibility of being a victim of phishing
	AV2:	If I can avoid thinking of being a victim of phishing, I will do that
	AV3:	I try to avoid thinking about the possibility of becoming a victim of phishing
Delayed avoidance (Witte et al., 1998)	AV4:	In the past month, I have often thought back to the text that I read
	AV5:	I have been thinking a lot about the text I have read over the past month
Message involvement (Shillair et al., 2015)	MI1:	I have read the text carefully
	MI2:	The text contains relevant information for me

Table B2: Pretest items (translated from Dutch)

Construct (sources)	Items	
Argument quality (De Hoog et al., 2005)	AQ1:	Strong arguments are used in the information provided
	AQ2:	The arguments used in the information provided are persuasive
	AQ3:	The information provided contains meaningful arguments
Issue derogation (Witte et al., 1998)	ID1:	The information in the text is exaggerated
	ID2:	The information in the text is overblown
Perceived manipulation (Witte et al., 1998)	MA1:	I feel that the information provided is manipulative
	MA2:	The information provided is misleading

The items of attitude are measured on a semantic differential scale based on the work of Davis (1993) and are operationalized as follows: The online sharing of personal information is: good (1) – bad (5); beneficial (1) – harmful (5); positive (1) – negative (5); wise (1) – foolish (5); favourable (1) – unfavourable (5).

Prior knowledge of phishing is based on the work of Shillair et al. (2015) and is asked as follows: To what extent are you familiar with phishing? Participants could answer this question in the following ways: I never heard of phishing; I have heard of phishing, but I do not understand the details; I know what phishing is, but I do not know what to do about it; I know what phishing is and how to protect myself against it.

Finally, we based the questions on internet experience and personal responsibility on previous work of Corbitt et al. (2003) and Boehmer et al. (2015) respectively. Internet experience was asked for by three different questions: (a) I have been using the internet for: less than 1 year; between 1 and 5 years; between 5 and 10 years; between 10 and 15 years; more than 15 years, (b) I use the internet approximately: less than 1 hour per week; between 1 and 3 hour per week; between 3 and 10 hours per week; between 10 and 20 hours per week; more than 20 hours per week, and (c) I perceive myself experienced at using the internet: 1 strongly disagree – 5 strongly agree. Personal responsibility was also measured on a 5-point Likert scale and was formulated as follows: I am primarily responsible for my safety on the internet.

Summary

This doctoral thesis is about the human aspects of online banking safety and security. Preparations for this thesis, part of The Dutch Research Program on Safety and Security of Online Banking, started when online banking fraud figures were relatively high in the Netherlands. In this thesis, online banking fraud is limited to phishing and malware attacks. This thesis investigated a specific part of the issue of how to reduce this type of fraud, namely the extent to which the safety and security of online banking can be improved from an end-user perspective. Hence, it examined how the online resilience of end users can be enhanced; making them better able to protect themselves against online banking fraud. Next to the practical goal of this thesis, it also aimed to contribute to scientific theory in the behavioural information security domain.

This thesis starts with an introductory Chapter (1) in which the context of study is described and the goal and research questions are highlighted. The empirical part of this thesis is divided into two smaller parts. In order to get a comprehensive overview of the human aspects of online banking safety and security, it is important to study the threats as well as people-focussed safeguards. Therefore, Part I (Chapters 2 to 5) deals with studies on end-users' perceptions of and victimization due to online banking fraud. Learning more about risk perceptions, how and why victimization takes place, victim characteristics and how victims recover from incidents may lead to more knowledge on how to combat online banking fraud effectively. Part II of this thesis (Chapters 6 to 9) consequently deals with studies on precautionary online behaviour of end users and how that behaviour can be improved. Knowledge on this subject may contribute to strengthening one of the most essential links in the safety and security of online banking: the end user. The concluding Chapter (10) provides an answer to the central and main research questions and deals with the theoretical and practical implications of the findings. The main research questions are:

1: What are the perceptions of end users regarding the safety and security of online banking?
2: How can online banking fraud victimization be explained from an end-user perspective?
3: How can precautionary online behaviour of end users be explained and improved?

To answer these questions, several studies were conducted; these are elaborated in Part I and Part II of this thesis. The contents of the chapters are outlined below.

In Chapter 2, end-user risk perceptions of online bank fraud are studied. Secondary analysis of data based on a survey among 1,200 Dutch online banking users shows that online banking fraud is not considered to be a major risk. End users perceive the potential impact of online banking fraud to be severe, but the chances of falling victim themselves to be slim. However, they estimate the chances of others being victimized to be higher. Furthermore, online banking customers mainly come into contact with online banking fraud through media communications. Indirect victimization in the social environment and direct victimization were less common. In addition, online banking users, in general, have reasonable levels of trust in online banking. Finally, this chapter reveals – using partial least squares path modelling – that risk perceptions are mainly affected by the estimated chance of becoming a victim of online banking fraud. The perceived impact of online banking fraud and the degree of trust in online banking affected risk perception to some extent. Direct and indirect victimization and demographic characteristics hardly affected risk perceptions.

In Chapter 3, an analysis of 600 phishing and malware incidents obtained from a Dutch bank is presented. The goal of this chapter is to shed light on the circumstances in which bank customers are victimized in phishing and malware attacks and how these attacks manifest in practice. This chapter shows that an essential step in the fraudulent process entails customers giving away their personal information to fraudsters. Phishing victimization mainly occurred by responding to a fraudulent e-mail, a fraudulent phone call or a combination of these. Malware victimization primarily occurred by responding to a malicious pop-up and by installing a malicious application on a mobile device. Customers cooperated because the fraudulent messages were perceived to be professional and trustworthy and because customers were not sufficiently suspicious of what was happening. The results suggest that victims have an unintended and subconscious, but active role in the fraudulent process. An interesting finding is that the victims did not always seem to trust the fraudster's intentions, but were mentally unable to stop the process. Reasons for this include not being aware of how fraudulent schemes manifest in practice, not being alert at the right moment and having insufficient knowledge of online banking procedures and precautionary measures.

Chapter 4 explores factors that may explain online banking fraud victimization based on interviews with 30 victims using the routine activity approach and protection motivation theory as theoretical lenses. A qualitative approach was

chosen because previous quantitative studies failed to identify such factors. The interview data were analysed using computer-assisted qualitative data analysis software. This chapter demonstrates that no specific factors from the routine activity approach and protection motivation theory that increase the chance of online banking fraud victimization could be identified. Moreover, victims were distributed across genders, age categories and levels of education. Ultimately, end-user attributes that lead to higher chances of being victimized through online banking fraud could not be identified. This suggests that everyone is susceptible to online banking fraud victimization to some degree.

In order to find out whether victims adequately recover from phishing and malware incidents, it is important to gain insight into its effects and impact on victims first. However, there was not much literature available on the impact of these cybercrimes. This gap is addressed in Chapter 5, in which interview data from the above mentioned 30 victims are analysed again. Besides (initial) financial effects (most victims were reimbursed), victims also described various kinds of psychological and emotional effects, such as feeling awful and stressed, and various kinds of secondary impact, such as time loss and not being treated properly during the handling of the incident. Furthermore, this chapter demonstrates that the level of impact varies among victims, ranging from little or no impact to severe impact. Moreover, while some victims were only affected for a few days, some felt the effects in the long term. The impact of these fraudulent schemes on victims should therefore not be underestimated.

In addition, the interview data provided insight into cognitive and behavioural change in order to cope with the incident. Cognitive strategies were mainly concerned with reducing psychological and emotional distress, and increasing online resilience to future attacks. The main behavioural strategies that were identified are reporting the incident to the bank and the police and seeking support from the social environment. Furthermore, various other actions were taken, such as enhancing the safety and security of devices and being more attentive during online banking sessions. However, it was observed that some of these actions were only of limited duration. Some victims adopted avoidance behaviours, such as making less use of online banking services. Victims who were left with financial damages rationalized the incident, thereby minimizing victimization for themselves. Chapter 5 concludes that the coping approach that was applied provides a useful framework to study the effects and impact of cybercrime victimization and how victims recover from it.

In Chapters 6 and 7, survey data on 1,200 Dutch online banking users are examined and analysed using partial least squares path modelling. In Chapter 6, three social cognitive models are compared with respect to their ability to

explain the intentions of precautionary online behaviour. The models are: protection motivation theory, the reasoned action approach and an integrated model comprising variables of these models. The three models were successfully applied to online banking. The individual models equally explain much of the variance in precautionary online behaviour. In the integrated model, the significant predictors of the two models remained significant and the level of explained variance was highest. Precautionary online behaviour is largely driven by response efficacy, self-efficacy and attitude towards that behaviour. This chapter concludes that both protection motivation theory and the reasoned action approach make a unique contribution in explaining variance for precautionary online behavioural intention. The integrated model explained most variance in protection motivation, which means that integrating theoretical perspectives from different domains is worthwhile. However, protection motivation theory is used as the main theoretical basis in the following chapters, because of its applicability to interventions.

Chapter 7 builds on the preceding chapter and continues to study a model of precautionary behaviour in the domain of online banking. The aim was to gain insight into factors that encourage customers to take measures to protect themselves against online threats. The analyses that were conducted for this chapter provided support for most of the hypothesized relationships and showed that the model explains high levels of variance for precautionary online behaviour as well as for risk perception. Threat and coping appraisal successfully predicted the protection motivation of online banking users; in particular, response efficacy and self-efficacy were the most important predictors for taking precautions. Secondary predictors include locus of control, perceived severity (direct effect) and the negative predictor response costs. Finally, some differences in precautionary online behavioural intentions were observed based on gender and level of education.

In Chapter 8, insight is gained into what protective measures self-employed entrepreneurs take in order to protect themselves against online threats and what motivates them to do so. Information technology is becoming increasingly important for entrepreneurs. Protecting their technical infrastructure and stored data is, therefore, also growing in importance. Nevertheless, research into the safety and security of entrepreneurs in general, and online threats targeted at entrepreneurs in particular, are still limited. Based on secondary analyses on data collected from 1,622 Dutch entrepreneurs, it was observed that the majority implement technical and personal coping measures. Entrepreneurs are likely to implement protective measures if they believe a measure is effective, if they are capable of using internet technology, if their attitude towards information security is positive and if they believe they are responsible for their

own online security. These findings are similar to those of private users outlined in Chapters 6 and 7. Finally, some differences in precautionary online behaviour were observed based on age and education level.

Chapter 9 examines the impact of fear appeal messages on user cognitions, attitudes, behavioural attentions and precautionary behaviour regarding online information-sharing to protect against the threat of phishing attacks. A pre-test post-test design was used in which 768 internet users filled out an online questionnaire. Participants were grouped in one of three fear appeal conditions: strong-fear appeal, weak-fear appeal and control condition. Claims regarding vulnerability of phishing attacks and claims concerning response efficacy of protective online information-sharing behaviour were manipulated in the fear appeal messages. This chapter demonstrates positive effects of fear appeals on heightening end-users' cognitions, attitudes and behavioural intentions. However, future studies are needed to determine how subsequent security behaviour can be promoted, as the effects on this crucial aspect were not directly observed. Nonetheless, fear appeals have great potential for promoting security behaviour by making end users aware of threats and simultaneously providing behavioural advice on how to mitigate these threats.

All things considered, this thesis investigated online banking fraud victimization and precautionary online behaviour. Specifically, human aspects were the focus of the present research. This thesis demonstrates that good security is in people's heads. It seems easier, cheaper and more successful for criminals to attack end users using psychology rather than the technology surrounding online banking. Hence, even the best security engineers cannot stop end users from giving away their security codes. Therefore, using psychology to defend against online banking attacks also makes sense. This is especially the case for attacks using social engineering (phishing), but to some extent also for attacks using technical engineering (malware). Considering the further digitization of our society and the increasing dependability on information systems, the case is made that people have to 'bend' with these developments and become resilient when online. This is necessary to stop people from 'breaking' and potentially becoming victims of online banking fraud.

While this thesis obtained information on how safety and security of online banking can be improved from an end-user perspective, it should be noted that end users will always be confronted with numerous potential threats. It is unrealistic to believe that people can protect themselves against all threats at all times. Therefore, we have to accept that bad things will continue to happen online, but optimistically they can be kept to a minimum if end users are more vigilant about what they do online and are aware of how some people abuse the

advantages that the internet offers. At the very least, the impact of these attacks can be reduced. The following main recommendations from this thesis may be helpful:

1: Continue to invest in security education, training and awareness campaigns concerning threats aimed at online banking.
2: Focus on underlying cognitive dimensions in security education, training and awareness campaigns, most notably on response efficacy and self-efficacy.
3: Make clear that banks and customers are partners in keeping online banking safe and secure.
4: Facilitate victims in their recovery process, primarily by providing feedback.
5: Continue with research on the human aspects of online banking safety and security.

In conclusion, security education, training and awareness remain an important priority, especially for combatting social risks. It is very important to promote online resilience. The research indicates that in order to strengthen the role of customers in the safety and security of online banking, threat appraisals as well as coping appraisals should be improved. If customers or end users believe that protective measures make a difference (response efficacy) and if they are able to perform these measures (self-efficacy), it is likely that end users will adopt precautionary behaviour and become a strong link in the information security chain. Proper information security practices should become part of our general skill set as people in this day and age. However, it should not be forgotten that safety and security is something that should be worked on together, with all parties involved. And when things do go wrong, we need to help one another to recover from it. All in all, an important requirement for a safer and more secure internet is that the human factor takes a central place in information security.

Samenvatting (summary in Dutch)

Buigen of barsten? Online bankfraude voorkomen door online weerbaarheid

Dit proefschrift gaat over de menselijke aspecten van de veiligheid van internetbankieren. De voorbereidingen voor dit proefschrift, onderdeel van het Kennisprogramma Veiligheid Digitaal Betalingsverkeer, zijn begonnen toen de online bankfraudecijfers relatief hoog waren in Nederland. Fraude met internetbankieren is hier beperkt tot phishing- en malware-aanvallen. In dit proefschrift is een specifiek deel onderzocht van de kwestie hoe dit type fraude te bestrijden, namelijk in welke mate de veiligheid van internetbankieren kan worden verbeterd vanuit het perspectief van de eindgebruiker. Of met andere woorden, hoe de online weerbaarheid van eindgebruikers kan worden vergroot; waardoor ze beter in staat zijn zichzelf te beschermen tegen online bankfraude.

Het proefschrift begint met een inleidend hoofdstuk (1) waarin de context van de studie wordt beschreven en de doelstelling en onderzoeksvragen worden belicht. Om een omvattend beeld te krijgen van de menselijke aspecten van de veiligheid van internetbankieren, is het belangrijk om zowel de risico's als mensgerichte veiligheidsmaatregelen te bestuderen. Derhalve is het empirische deel van dit proefschrift opgedeeld in twee delen. In Deel I (hoofdstukken 2 t/m 5) staan percepties van eindgebruikers over risico's van internetbankieren en slachtofferschap van online bankfraude centraal. Meer kennis over risico-percepties, hoe en waarom slachtofferschap plaatsvindt, slachtofferkenmerken en hoe slachtoffers herstellen van incidenten geeft meer inzicht in hoe online bankfraude effectief kan worden bestreden. In Deel II (hoofdstukken 6 t/m 9) worden studies over veilig online gedrag van eindgebruikers behandeld en hoe dit gedrag kan worden verbeterd. Kennis over dit onderwerp draagt bij aan het versterken van een van de meest essentiële schakels in de veiligheidsketen van internetbankieren: de mens. In het afsluitende hoofdstuk (10) worden de onderzoeksvragen beantwoord en wordt stil gestaan bij de theoretische en praktische implicaties van de bevindingen. De belangrijkste onderzoeksvragen in dit onderzoek zijn:

1: Wat zijn de percepties van eindgebruikers over de veiligheid van internetbankieren?

2: Hoe kan slachtofferschap van online bankfraude worden verklaard vanuit een gebruikersperspectief?

3: Hoe kan veilig online gedrag van eindgebruikers worden verklaard en verbeterd?

Om deze vragen te beantwoorden, zijn verschillende onderzoeken uitgevoerd; ondergebracht in Deel I en Deel II van dit proefschrift. De inhoud van de hoofdstukken is hieronder nader uitgewerkt.

In hoofdstuk 2 worden risicopercepties van eindgebruikers met betrekking tot online bankfraude bestudeerd. Secundaire analyse van vragenlijstdata van 1.200 Nederlandse gebruikers van internetbankieren laat zien dat fraude met internetbankieren niet als een groot risico wordt ervaren. Eindgebruikers ervaren de mogelijke impact van online bankfraude als ernstig, maar de kans om zelf slachtoffer ervan te worden als klein. Ze schatten de kans dat anderen slachtoffer worden hoger in. Daarnaast horen gebruikers van internetbankieren vooral in de media over online bankfraude. Indirect slachtofferschap in de sociale omgeving en direct slachtofferschap komen minder vaak voor. Bovendien hebben gebruikers van internetbankieren over het algemeen een behoorlijke mate van vertrouwen in internetbankieren. Tot slot laat dit hoofdstuk zien – door middel van padanalyse – dat risicopercepties vooral worden beïnvloed door de ingeschatte kans om slachtoffer te worden van fraude met internetbankieren. De waargenomen impact van online bankfraude en de mate van vertrouwen in internetbankieren beïnvloeden de risicoperceptie tot op zekere hoogte. Direct en indirect slachtofferschap en demografische kenmerken beïnvloeden de risicoperceptie nauwelijks.

In hoofdstuk 3 zijn 600 phishing- en malwarezaken van een Nederlandse bank geanalyseerd. Het doel van dit hoofdstuk is om inzicht te krijgen in de omstandigheden rond bankklanten die het slachtoffer zijn van phishing- en malware-aanvallen en hoe deze aanvallen zich in de praktijk manifesteren. Dit hoofdstuk laat zien dat een essentiële stap in het frauduleuze proces is dat klanten hun persoonlijke informatie weggeven aan fraudeurs. Het gaat daarbij voornamelijk om beveiligingscodes. Slachtofferschap van phishing vindt voornamelijk plaats door te reageren op een valse e-mail, een frauduleus telefoontje of een combinatie hiervan. Malware-slachtofferschap vindt veelal plaats door te reageren op een valse pop-up en door een kwaadaardige applicatie op een mobiel apparaat te installeren. Klanten reageerden hierop omdat de frauduleuze berichten professioneel en betrouwbaar overkwamen en omdat ze niet voldoende achterdochtig waren voor wat er gebeurde. De resultaten suggereren dat slachtoffers een onbedoelde en onbewuste, maar actieve rol hebben in het frauduleuze proces. Een interessante bevinding is dat de slachtoffers niet altijd de intentie van de fraudeur leken te vertrouwen, maar mentaal niet in staat waren om het proces te stoppen. Redenen hiervoor zijn het zich niet bewust zijn van hoe frauduleuze handelingen zich in de praktijk voltrekken, niet alert zijn op het juiste moment en onvoldoende kennis hebben van procedures voor internetbankieren en van beschermende maatregelen.

In hoofdstuk 4 is aan de hand van interviews met 30 slachtoffers onderzoek gedaan naar factoren die het slachtofferschap van online bankfraude kunnen verklaren. Hiervoor zijn de *routine activity approach* en de *protection motivation theory* als theoretische kapstok gebruikt. Er is gekozen voor een kwalitatieve benadering, omdat eerdere kwantitatieve studies dergelijke factoren niet konden identificeren. De interviewdata zijn geanalyseerd met behulp van kwalitatieve data-analysesoftware. Dit hoofdstuk laat zien dat er geen specifieke factoren uit de toegepaste theorieën kunnen worden geïdentificeerd die de kans vergroten op slachtofferschap van online bankfraude. Bovendien zijn slachtoffers verdeeld over sekse, leeftijd en opleidingsniveau. Uiteindelijk kunnen kenmerken van eindgebruikers die leiden tot een grotere kans om slachtoffer te worden van fraude met internetbankieren niet worden geïdentificeerd. Dit suggereert dat iedereen tot op zekere hoogte gevoelig is voor slachtofferschap van online bankfraude.

Om erachter te komen of slachtoffers adequaat herstellen van phishing- en malware-incidenten, is het van belang om eerst inzicht te krijgen in de effecten en impact op slachtoffers. Literatuur over de impact van deze vormen van cybercriminaliteit is echter schaars. Dit hiaat wordt behandeld in hoofdstuk 5, waarin interviewgegevens van dezelfde 30 slachtoffers nader zijn geanalyseerd. Naast (aanvankelijke) financiële gevolgen (de meeste slachtoffers werden schadeloos gesteld) beschreven slachtoffers ook verschillende vormen van psychologische en emotionele effecten, zoals zich beschaamd en gestrests voelen, en verschillende soorten secundaire gevolgen, zoals tijdverlies en niet goed worden behandeld bij de afhandeling van het incident. Verder laat dit hoofdstuk zien dat de mate van impact die slachtoffers ervaren varieert van weinig of geen impact tot zeer veel impact. Bovendien komt naar voren dat sommige slachtoffers slechts een paar dagen last hadden van dergelijke effecten terwijl sommigen nadelige gevolgen ondervonden op de lange termijn. De impact van frauduleuze incidenten op slachtoffers moet daarom niet worden onderschat.

Verder wordt in dit hoofdstuk inzicht gegeven in veranderingen die slachtoffers doormaken naar aanleiding van het incident. Cognitieve strategieën hebben vooral betrekking op het verminderen van psychologische en emotionele stress en het vergroten van online weerbaarheid met betrekking tot toekomstige aanvallen. De belangrijkste gedragsstrategieën die zijn geïdentificeerd zijn het rapporteren van het incident aan de bank en de politie en het zoeken van steun vanuit de sociale omgeving. Verder zijn verschillende andere acties ondernomen door de slachtoffers, zoals het verbeteren van de beveiliging op de apparaten die gebruikt worden voor internetbankieren en het meer alert zijn tijdens internetbankiersessies. Echter, sommige van deze acties waren slechts van korte

duur. Daarnaast gaven sommige slachtoffers aan vermijdingsgedrag te vertonen, zoals het minder gebruik maken van internetbankieren. Slachtoffers waarvan de financiële schade niet werd gecompenseerd, rationaliseerden het incident en minimaliseerden daarmee het slachtofferschap voor zichzelf. In hoofdstuk 5 wordt geconcludeerd dat de toegepaste *coping*-aanpak een bruikbaar kader biedt voor het bestuderen van de effecten en impact van cybercrimeslachtofferschap en hoe slachtoffers daarvan herstellen.

In hoofdstukken 6 en 7 zijn vragenlijstdata van 1.200 Nederlandse gebruikers van internetbankieren geanalyseerd met behulp van padanalyse. In hoofdstuk 6 zijn drie sociaal-cognitieve modellen vergeleken in hun vermogen om de intenties van veilig online gedrag te verklaren. De modellen zijn: *protection motivation theory*, *reasoned action approach* en een geïntegreerd model met variabelen uit deze modellen. De drie modellen zijn met succes toegepast op de internetbankieren-context. De individuele modellen verklaren ongeveer evenveel van de variantie in veilig online gedrag. In het geïntegreerde model bleven de voorspellers van de twee modellen significant en was het niveau van de verklaarde variantie het hoogst. Veilig online gedrag wordt grotendeels bepaald door de ingeschatte responseffectiviteit, zelfeffectiviteit en de houding ten opzichte van dat gedrag. In dit hoofdstuk wordt geconcludeerd dat zowel de *protection motivation theory* als de *reasoned action approach* een unieke bijdrage leveren aan het verklaren van de variantie voor veilig gedrag op internet. In de volgende hoofdstukken wordt de *protection motivation theory* als belangrijkste theoretische basis gebruikt vanwege de toepasbaarheid ervan op interventies.

Hoofdstuk 7 bouwt voort op het vorige hoofdstuk en werkt verder aan een model van veilig online gedrag op het gebied van internetbankieren. Het doel was om inzicht te krijgen in factoren die klanten beïnvloeden om beschermende maatregelen te treffen tegen online dreigingen. De analyses die voor dit hoofdstuk zijn uitgevoerd, ondersteunen de meeste hypothesen en laten een hoge mate van verklaarde variantie zien voor zowel veilig online gedrag als voor risicoperceptie. Beide cognitieve processen die centraal staan in de *protection motivation theory*, namelijk *threat appraisal* (evaluatie van de ingeschatte dreiging) en *coping appraisal* (evaluatie van mogelijke strategieën om met een dreiging om te gaan) voorspellen de protectiemotivatie van eindgebruikers. De belangrijkste voorspellers voor veilig online gedrag zijn responseffectiviteit en zelfeffectiviteit. Secundaire voorspellers zijn *locus of control*, gepercipieerde impact (direct effect) en responskosten. Ten slotte werden enkele verschillen in motivaties voor veilig online gedrag waargenomen met betrekking tot sekse en opleidingsniveau.

In hoofdstuk 8 wordt inzichtelijk gemaakt welke maatregelen zelfstandigen zonder personeel (hierna: ondernemers) nemen om zichzelf te beschermen tegen online dreigingen en wat hen motiveert om dit te doen. Informatie-technologie wordt steeds belangrijker voor ondernemers. Het beschermen van hun technische infrastructuur en bedrijfsgegevens worden daarmee ook steeds belangrijker. Desalniettemin is onderzoek onder ondernemers naar de veiligheid of beveiliging in het algemeen en online dreigingen in het bijzonder schaars. Op basis van een secundaire analyse van vragenlijstdata van 1.622 Nederlandse ondernemers, is inzichtelijk gemaakt dat de meerderheid van de ondernemers technische en persoonlijke *coping*-maatregelen treft. Dit hoofdstuk laat zien dat de waarschijnlijkheid dat ondernemers beschermende maatregelen treffen het hoogst is wanneer zij menen dat een maatregel effectief is, wanneer zij in staat zijn om internettechnologie te gebruiken, wanneer hun houding tegenover informatiebeveiliging positief is en wanneer zij geloven dat zij verantwoordelijk zijn voor hun eigen online veiligheid. Deze bevindingen zijn vergelijkbaar met die van de particuliere doelgroep in hoofdstukken 6 en 7. Ten slotte zijn enkele verschillen in veilig gedrag waargenomen met betrekking tot leeftijd en opleidingsniveau.

In hoofdstuk 9 wordt verslag gedaan van een onderzoek naar de impact van *fear appeals* op cognities, attitudes, intenties en gedrag van internetgebruikers met betrekking tot het online delen van informatie ter bescherming tegen phishing-aanvallen. Een *pre-test post-test design* is toegepast waarbij 768 internet-gebruikers een online vragenlijst invulden. Deelnemers werden gegroepeerd in een van de drie *fear appeal* condities: een conditie met sterke argumenten, een conditie met zwakke argumenten en een controle conditie; zonder *fear appeal*. Argumenten gericht op persoonlijke kwetsbaarheid van phishing-aanvallen en argumenten gericht op de responseffectiviteit van veilig gedrag met betrekking tot het online delen van persoonlijke informatie werden gemanipuleerd in de *fear appeal* berichten. Dit hoofdstuk laat positieve effecten van *fear appeals* zien op het verhogen van de cognities, attitudes en gedragsintenties van internet-gebruikers. Vervolgonderzoek is echter nodig om te bepalen hoe het daadwerkelijke gedrag kan worden bevorderd, omdat de effecten op dit cruciale aspect niet direct werden waargenomen. Desalniettemin hebben *fear appeals* een groot potentieel om veilig online gedrag te bevorderen door internet-gebruikers bewust te maken van dreigingen en tegelijkertijd een concreet advies te geven over hoe deze dreigingen kunnen worden beperkt.

In dit proefschrift is onderzoek gedaan naar slachtofferschap van online bankfraude en veilig online gedrag. Specifiek waren menselijke aspecten de focus van het huidige onderzoek. Dit proefschrift laat zien dat goede beveiliging in de hoofden van mensen zit. Het lijkt eenvoudiger, goedkoper en succesvoller

voor criminelen te zijn om eindgebruikers aan te vallen met behulp van psychologie in plaats van de technologie rondom internetbankieren. De knapste koppen op het gebied van informatiebeveiliging kunnen niet voorkomen dat eindgebruikers hun beveiligingscodes weggeven. Daarom is het logisch om in de verdediging tegen aanvallen op internetbankieren ook gebruik te maken van psychologie. Dit is vooral het geval voor *social engineering* aanvallen (phishing), maar in zekere mate ook voor *technical engineering* aanvallen (malware). Gezien de verdere digitalisering van onze samenleving en de toenemende afhankelijkheid van informatiesystemen, is het zaak dat mensen mee 'buigen' met deze ontwikkelingen en online weerbaar worden. Dit is nodig om te voorkomen dat mensen 'barsten' en mogelijk het slachtoffer worden van fraude met internetbankieren.

Hoewel met dit proefschrift inzicht is verkregen in hoe de veiligheid van internetbankieren kan worden verbeterd vanuit het perspectief van de eindgebruiker, moet worden opgemerkt dat eindgebruikers voortdurend worden geconfronteerd met tal van potentiële dreigingen. Het is een utopie om te geloven dat mensen zich te allen tijde kunnen beschermen tegen alle dreigingen. Daarom moeten we accepteren dat slachtofferschap van online bankfraude zal blijven bestaan, maar – vanuit een optimistische kijk op de zaak – wel tot een minimum kan worden beperkt. Met name wanneer eindgebruikers meer alert zijn op wat ze doen online en zich bewust zijn van hoe sommige mensen de mogelijkheden van het internet misbruiken. Op zijn minst kan de impact die door deze aanvallen wordt veroorzaakt worden verminderd. De volgende hoofdaanbevelingen uit dit proefschrift kunnen hieraan bijdragen:

1: Blijf investeren in educatie, training en bewustwordingscampagnes rond dreigingen gericht op internetbankieren.
2: Focus op onderliggende cognitieve dimensies in educatie, training en bewustwordingscampagnes, met name op responseffectiviteit en zelfeffectiviteit.
3: Maak duidelijk dat banken en klanten partners zijn in het veilig houden van internetbankieren.
4: Faciliteer slachtoffers in hun herstelproces, voornamelijk door feedback te geven.
5: Ga door met onderzoek naar de menselijke aspecten van de veiligheid van internetbankieren.

Concluderend, veiligheidseducatie, training en het vergroten van awareness blijven een prioriteit, vooral voor het bestrijden van sociale risico's. Het is belangrijk om online weerbaarheid te stimuleren. Uit onderhavig onderzoek blijkt dat om de rol van eindgebruikers in de veiligheid van internetbankieren te versterken zowel de *threat appraisal* als de *coping appraisal* moet worden aangewakkerd. Wanneer bankklanten of eindgebruikers zich bewust zijn van een dreiging en geloven dat beschermende maatregelen daadwerkelijk een verschil maken (responseffectiviteit) en ze in staat zijn om deze maatregelen uit te voeren (zelfeffectiviteit) dan is het waarschijnlijk dat eindgebruikers voorzorgsmaatregelen zullen treffen en een sterke schakel vormen in de informatiebeveiligingsketen. Gezien de huidige tijdsgeest zou goed informatiebeveiligingsgedrag deel moeten uitmaken van onze algemene vaardigheden. We mogen echter niet vergeten dat (online) veiligheid een onderwerp is dat samen met alle betrokken partijen moeten worden aangepakt. En wanneer er toch iets fout gaat, dan moeten we elkaar helpen om daarvan te herstellen. Al met al is een belangrijke vereiste voor een veiliger internet dat de menselijke factor een centrale plaats inneemt in de informatiebeveiliging.

Dankwoord (acknowledgements in Dutch)

Tijdens de eerste drie jaar van mijn werkzaamheden voor het lectoraat Cybersafety van NHL Stenden Hogeschool en Politieacademie heb ik veel kennis opgedaan over cybersafety- en cybercrimevraagstukken en heb ik mijn vaardigheden in het doen van onderzoek kunnen ontplooien. In 2013 kwam de kans voorbij om te starten met een promotieonderzoek naar de veiligheid van internetbankieren met als uitgangspunt de eindgebruiker. Een onderzoek naar een zeer interessant en actueel onderwerp waarin de mens als centraal uitgangspunt wordt genomen was mij op het lijf geschreven.

In de afgelopen vier jaar is er een hoop gebeurd. Hoewel de directe urgentie van phishing- en malware-aanvallen op het internetbankieren in Nederland lijkt af te nemen is het vraagstuk naar het digitaal weerbaar maken van internetgebruikers nog steeds een zeer relevant en actueel thema. Hoewel het natuurlijk nooit helemaal is in te schatten hoe onderzoeksresultaten landen, hoop ik dat dit onderzoek bijdraagt aan het versterken van de belangrijkste schakel in de informatiebeveiliging: de mens.

Het proefschrift dat voor u ligt was niet mogelijk zonder de hulp en steun van velen. Daarom wil ik een aantal personen expliciet bedanken voor hun bijdrage bij de totstandkoming van dit product.

Laat ik beginnen met mijn promotor en copromotor. Wouter, bedankt voor de kans die je me hebt gegeven om mij te storten op dit project. De verantwoordelijkheid en vrijheid die je me toevertrouwde om dit project uit te voeren, zorgen ervoor dat ik met genoegen terug kijk op mijn tijd als promovendus. Ook ben ik je dankbaar voor je scherpe feedback als ik weer eens iets had geschreven. Nicolien, bedankt voor de gesprekken die we voerden over de voortgang van het onderzoek en de immer interessante ontwikkelingen die gaande zijn bij de Nationale Politie en Politieacademie. Door jouw enthousiasme bleef ik vertrouwen houden in de voortgang van mijn promotietraject.

Daarnaast kan ik er niet om heen om mijn *partners in science* te noemen. Promovendus zijn is van tijd tot tijd een behoorlijk solistische aangelegenheid. Daarom prijs ik mij gelukkig dat het promotieonderzoek onderdeel was van het Kennisprogramma Veiligheid Digitaal Betalingsverkeer waarin vier promovendi werkten aan hun promotieonderzoek. Rutger, Sanne en Sven, ik heb veel aan jullie gehad. De vele uitwisselingen van gedachten, het lezen van elkaars stukken, inspirerende ‘bosdagen’, interessante congresbezoeken, etentjes en de vele bakjes ‘goede koffie’ zorgden ervoor dat het promotietraject een plezier was om af te leggen.

Ook de aanmoediging van mijn collega's van het lectoraat (Joyce, Sander, Renske, Ton, Willem, Marja, Suzanna, Saskia, Bram en de vele stagiairs), van mijn collega's uit het kennisprogramma (Evert en Marko) en van verschillende collega's van de Thorbecke Academie en het NHL PhD-Netwerk (bestuur) heb ik als zeer prettig ervaren, waarbij ik Marieke en Marika niet ongenoemd wil laten. Het stellen van geïnteresseerde vragen en het meedenken over de materie hebben dit product beter gemaakt. De informele sfeer, humor en gezelligheid die jullie ook brachten, zorgden ervoor dat ik met genoegen bleef knutselen aan mijn onderzoek. Dank jullie wel voor de vele leuke momenten.

Een volgend woord van dank gaat uit naar Paul. Al maakte je niet direct onderdeel uit van het kennisprogramma, je bijdrage is van zeer grote waarde geweest. Paul, bedankt voor het meedenken in de ontwerpfase van de onderzoeken naar protectiemotivatie, de ongekende snelheid waarmee je reageerde op verschillende vraagstukken en voor het delen van je kennis en expertise op het gebied van de complexere statistische analyses. Dankzij jou heb ik mij de analysemethode PLS-SEM snel eigen kunnen maken. Bovendien heeft onze samenwerking geleid tot mooie publicaties waarvan er een aantal zijn opgenomen in dit proefschrift. Ik hoop dat we onze vruchtbare samenwerking kunnen blijven voortzetten in de toekomst.

Dit project was niet mogelijk zonder financiering van de bancaire sector – vertegenwoordigd door de Nederlandse Vereniging van Banken –, de Politieacademie en de Nationale Politie. Ik wil de opdrachtgevers dan ook bedanken voor de mogelijkheid die zij hebben geboden voor dit onderzoek om doorgang te vinden. Daarnaast wil ik de leden van de stuurgroep (Rob, Dave, Peter, Han, Eileen, Roel, Yvonne en Nicole) en de klankbordgroep (onder leiding van Stavros) bedanken voor het meedenken en discussiëren over (de inhoud van) het onderzoek. Speciale dank gaat uit naar diegenen – zowel binnen als buiten de projectorganisatie – die tijd konden vrij maken in hun volle agenda's om met mij over de verschillende deelonderzoeken te brainstormen of mij op andere wijze konden faciliteren. Mariëlle, Marijke en Astrid ben ik daar in het bijzonder erkentelijk voor.

Tevens wil ik alle respondenten bedanken die op welke manier dan ook hebben meegewerkt aan mijn onderzoek. Speciale aandacht gaat daarbij uit naar de respondenten die aan hun keukentafel, in hun woonkamer of op hun werkplek allerlei intieme details hebben gedeeld over het fraude-incident dat ze hebben meegemaakt en de impact die dat had op hun persoonlijke leven. Daarbij mag ik de contactpersonen binnen de politie en de Fraudehelpdesk die hebben bemiddeld in het benaderen van deze mensen niet vergeten. Jan Douwe en Lotte, heel erg bedankt voor jullie inzet.

Ook wil ik de leden van de beoordelingscommissie bedanken voor hun bereidheid om plaats te nemen in deze commissie en om mijn proefschrift kritisch te lezen en te boordelen.

Naast de promotor, copromotor, collega's en zakelijke relaties wil ik nog aantal personen uit de privésfeer bedanken. Hoewel zij niet directe inbreng hebben geleverd aan het proefschrift, hebben ze dit proefschrift wel mede mogelijk gemaakt. Het is mede dankzij hun succeswensen dat ik het proefschrift op tijd heb afgekregen. Heit en mem, bedankt voor jullie steun en vertrouwen die jullie altijd hebben uitgesproken. Cornelis en Sybren, bedankt voor het terzijde staan van jullie broer tijdens de verdediging van zijn proefschrift. Erkenning gaat ook uit naar de rest van de familie, waarbij ik mijn zusje Botsy expliciet wil noemen. Ook het tennisteam mag hier niet ontbreken. Het samen toewerken naar de volgende overwinning heeft mij mentaal scherp gehouden. En natuurlijk gaat er dankbaarheid uit naar de vriendengroep die een belangrijke rol speelt in de momenten van vermaak en ontspanning. Het is altijd goed jullie te zien en een biertje te drinken.

Tot slot wil ik Bianca bedanken voor de morele support. Bianca, als er iemand de afgelopen vier jaar naar mijn promotieverhalen heeft moeten luisteren dan ben jij het wel. Bedankt voor je oprechte interesse in mijn onderzoek en voor het bieden van een luisterend oor op de juiste momenten. Maar boven dat ben ik je dankbaar dat je mij het mooiste hebt geschonken wat ik me maar kan wensen: onze lieve dochter Féline! Met jouw komst is het een stuk eenvoudiger geworden om te relativeren.

Bedankt allemaal en oan't sjen!

Jurjen

Curriculum vitae

Jurjen Jansen (1983) obtained his bachelor's degree in Communication and Multimedia Design at the NHL University of Applied Sciences in 2005, and his master's degree in Communication Studies at the University of Twente in 2007, where he specialised in new media, research and design. From 2007 to 2010, Jurjen worked as a researcher on topics concerning electronic government at the Faculty of Behavioural Sciences at the University of Twente.

Since 2010, Jurjen has been working for the Cybersafety Research Group at the NHL Stenden University of Applied Sciences and the Dutch Police Academy. As a researcher, he has worked on projects on youth and cybersafety, the nature and extent of cybercrime among Dutch citizens and the digital security of small and medium-sized enterprises. In addition, he assists students in designing and conducting research. In 2013, Jurjen started working on a PhD project on strengthening the online resilience of end users. He conducted his research at the same department within NHL Stenden and was facilitated by the Open University of the Netherlands. This thesis is the result of a four-year endeavour. The project has resulted in several publications in various national and international peer-reviewed academic journals and conference proceedings. Moreover, he has actively contributed to the debate on the human aspects of information security at various national and international conferences.

Jurjen plans to continue his work in the field of behavioural information security in general and more specifically on online resilience of end users.

Publications

Publications in this thesis (in order of appearance):

Jansen, J., Kop, N. & Stol, W. (2017). Internetbankieren: Veiligheidspercepties van gebruikers [End-user perceptions of safety and security of online banking]. *Tijdschrift voor Veiligheid*, *16*(1), 36–51.

Jansen, J. & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In *Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust (STAST),* 13 July, Verona (Italy), pp. 24–31.

Jansen, J. & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology, 10*(1), 79–91.

Jansen, J. & Leukfeldt, R. (accepted). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice & Criminology*.

Jansen, J. & Schaik, P. van (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security, 25*(2), 165–180.

Jansen, J. & Schaik, P. van (submitted). Testing a model of precautionary online behaviour: The case of online banking.

Jansen, J., Veenstra, S., Zuurveen, R. & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology, 35*(5), 368–379.

Jansen, J. & Schaik, P. van (submitted). The design and evaluation of a theory-based intervention to promote security behaviour against phishing.

Other publications related to the research program:

Journal articles

Jansen, J. & Schaik, P. van (accepted). Persuading end users to act cautiously online: A fear appeals study on phishing. *Information & Computer Security.*

Leukfeldt, R. & Jansen, J. (2015). Cybercriminal networks and money mules: An analysis of low-tech and high-tech fraud attacks in the Netherlands. *International Journal of Cyber Criminology, 9*(2), 173–184.

Conference papers

Jansen, J. (2015). Studying safe online banking behaviour: A protection motivation theory approach. In *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA),*1-3 July, Mytilene (Greece), pp. 120–130.

Jansen, J. & Schaik, P. van (2016). Understanding precautionary online behavioural intentions: A comparison of three models. In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, 19-21 July, Frankfurt (Germany), pp. 1–11.

Jansen, J. & Schaik, P. van (2017). Persuading end users to act cautiously online: Initial finding of a fear appeals study on phishing. In *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA),* 28-30 November, Adelaide (Australia), pp. 1–11.

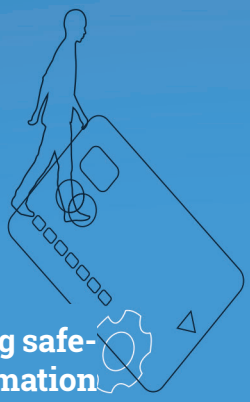
Conference abstracts

Jansen, J. (2015). *Slachtofferschap van phishing en malware gericht op internetbankieren* [Victims of phishing and malware attacks on online banking]. Nederlandse Vereniging voor Criminologie (NVC) Congres, 11-12 June, Leiden (the Netherlands), p. 125.

Jansen, J. & Schaik, P. van (2016). *Prevention of online banking fraud: An end-user perspective*. EUROCRIM Conference, 21-24 September, Münster (Germany), p. 487.

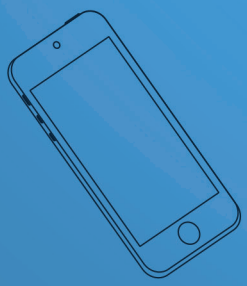
Conference poster

Jansen, J. & Kiljan, S. (2015). *Safety and security of online banking*. EUROCRIM Conference, 2-5 September, Porto (Portugal), pp. 815–816.



This thesis is about the human aspects of online banking safety and security. End users are a central link in the information security chain, for online banking too. Despite technical security measures, security codes sometimes unintentionally fall into the hands of perpetrators, for instance, through successful phishing and malware attacks. This allows perpetrators to steal money from private and corporate bank accounts. Therefore, it is important to make end users resilient when online, in an effort to combat these attacks on online banking.

This thesis presents several studies that contribute to making end users online resilient and is divided into two empirical parts. The first part describes four studies that investigated risk perceptions and online banking fraud victimization. The second part describes four studies that investigated precautionary online behaviour and how that behaviour can be influenced for the better. Researchers in the field of behavioural information security and practitioners in the field of security education, training and awareness can use the insights from this thesis in their line of work, to examine the issues more thoroughly and to maximize the effectiveness of security campaigns respectively.



Open Universiteit
www.ou.nl

NHL STENDEN
university of
applied sciences

POLITIE
Politieacademie